

Blockchain Medicine Administration Records (BMAR): Reflections and Modelling Blockchain with UML



Ian Mitchell

Abstract Modelling blockchain should be easy? There are many figures and diagrams that are intuitive, however they are often unorthodox and do not comply with standard modelling techniques, e.g., UML. The enterprise blockchain system designed is for Medicines Administration Records (MARs) and requires audits for accreditation, that exposes vulnerabilities to unauthorised access and alteration. These alterations are made in order to pass inspection of the auditors and often completed to correct human errors unforeseen until the audit. The design stage has *five* stages and includes *four* stages from UML. The initial stage looks at how effective blockchain is as a solution for the problem domain, and then followed by Use Case, Sequence, State Machine and Deployment. The final design was implemented and the overall approach is evaluated.

Keywords Blockchain modelling · Permissioned blockchain · Blockchain development · Medication administration records · Medication administration errors

1 Introduction

The ability to model before building is strategic to any engineering domain. Blockchain engineering is no different, and blockchain modelling has produced many illustrations that are intuitive and bespoke. The diagrams are different and unorthodox to other software engineering practices. The approach taken here utilises and tries to adapt existing models to blockchain engineering project in healthcare, Blockchain Medicines Administration Records, or BMARs [1] for short. So, the problem is twofold: (i) develop a blockchain consortium for BMARs; and, (ii) understand the issues with modelling blockchain with UML. The next section introduces the problem domain and the rest of the paper looks at how to model this as a blockchain using UML notation.

I. Mitchell (✉)
Middlesex University, London, UK
e-mail: i.mitchell@mdx.ac.uk

2 Problem Domain

Falsification of documentation or records is something that healthcare professionals deny publicly, but privately there are issues. Healthcare professionals have to complete equipment checks, document the administration of medication and its reactions to patients, and many other processes that all require auditing by some central governing quality assurance agency. The evidence is anecdotal that falsification occurs, and only comes to light when there are whistle-blowers or the patient makes a litigation. The temptation when a lawsuit is issued, is to amend, edit or destroy the documentation and to retrospectively contaminate the evidence in favour of the defendant. Whilst rare, there are cases that indicate that this occurs and how tragic the consequences are [2]. In this case the U.S. supreme court decided that the destruction and alteration of medical records by a paediatrician was to evade the potential medical malpractice that could have followed.

It is not only paediatricians or General Practitioners, that can spoliage evidence or make mistakes. All healthcare professionals have opportunities to do this. Removing this opportunity, promotes trust between all parties, and is the ambition of BMARs [1]. Briefly, BMARs uses blockchain to automate and audit the completion of Medicines Administration Records, see [3] for further information on advice on MARs completion.

2.1 Blockchain

Permissioned blockchain development is inspired by the work of [4], and relies on append-only decentralised ledgers, but this is where the similarities stop. Permissioned blockchain development does not require Practical Byzantine Fault Tolerance, PBFT [5, 6], since all the parties involved in the blockchain development channel are to be trusted and therefore requires only fault tolerance. This difference allows faster and more efficient consensus algorithms since they do not have to ascertain trust between each party. This in turn sees increased throughput in updating the blockchain and reduces the energy expended. The other differences are: (i) that permissioned blockchains are written in Turing complete languages, e.g., Java, and is therefore deterministic; and (ii) tokens or crypto-currency is optional.

So far, so good but what about patient privacy and confidentiality, surely this can be compromised on a network? This final point is significant and important to all healthcare professionals, if we are going to use blockchain technology to overcome this, the question of security and service-user (SU) privacy and confidentiality has to arise. This will be looked at in more detail, but essentially the same technology that keeps transactions anonymous on a permissionless blockchain, e.g., bitcoin, is used to keep information secure and private on a permissioned blockchain.

2.2 Medicines Administration Records, MARs

The motivation is to prevent falsification of documentation. Falsification can include, the destruction, editing, overwriting, and any other means of altering the medical data. The solution is to use permissioned blockchain technology to medical data. The problem domain is still required, one of the simple tasks that healthcare professionals have to complete when administering drugs to service users (SU), is the use of a MARs sheet. The MARs sheet records when an SU receives medication and their reaction to it. It can also record the refusal to take medication and the method in which it was applied. Guidance on completion of MARs sheets includes the 6 R's [7], which are:

1. right resident,
2. right medicine,
3. right route,
4. right dosage,
5. right time; and,
6. right to refuse.

The MARs sheet is preserved and included in quality assurance inspections. For the UK this is completed by the Care Quality Commission, CQC, which is the accrediting body for all healthcare providers, including care homes. So, the problem definition is to design and model a permissioned blockchain application that implements MARs.

The rest of this paper is divided up into, Sect. 3 the method and approach used to model blockchain, Sect. 4 the evaluation of the system and Sect. 5 discusses the issues and summarises the approached used.

3 Method

For reasons aforementioned, permissioned blockchain is conducive to implement applications that deal with medical data or records. There are many blockchain medical applications, e.g., see [8–10] that handle medical data. From these, and other applications it is known that auditability is apt for blockchain; and, e-Health Records (EHR) can be stored on blockchain, without contravening any of the Caldicott principles [11, 12]. However, the first stage of any design is to ask if blockchain is a suitable solution? This is not a feasibility study but a quick review to decide if blockchain technology is conducive to solving the given problem. In technology, buzzwords and trends sometimes overrule common sense, in the 1990s everything was Web 1.0 and everyone wanted a website. Web 2.0 saw everything shift to user-content generation, or/and social media, again the applications of this had huge success but also saw many instances of Web 2.0 backfire on organisations. Web 3.0 [13] is blockchain or decentralised ledgers, and the advantage is that the mistake of using gratuitous

technical solutions to problems that are solved has been done in Web 1.0 and 2.0—it is the intention of Web 3.0 not to make the same mistakes.

3.1 *Blockchain Efficacy Analysis*

So, when designing a decentralised application, be it permissioned or permissionless, there are some guidelines to see if your problem domain is conducive to blockchain. This simple set of guidelines can be found as a flowchart in [24, p. 57]. There are six questions, adapted from [14], that are going to be answered below for BMARs:

Need a shared consistent data store? According to Oscar Research [15] there are over 20,000 care homes registered in the UK. Whilst not all of these may have facilities or trained personnel to administer medicines, many of them will, e.g., 5028 are Nursing Homes. There is not so much a need to share data across a community of care homes, however there is a need to share data with the auditors. So, yes there is a need to share consistent data with auditor.

More than one participant to contribute data? In each care home there are multiple SUs, across a single country there are multiple care homes. There is not an exact number available in the UK, but if only 10% of the care homes used MAR sheets, then everyday there would be at least 2,000 records produced. All could be subject to falsification or errors. So, yes more than one participant would contribute data.

Data records are never updated or deleted? These records should never be edited or deleted. Even after the SU's death these anonymous records would remain for relevant investigations. MAR sheets themselves should never be altered or edited in anyway. The information about participants, Care Home Providers (CPH), prescriptions and medication are stored on a database—these already exist. The blockchain, via a secure channel, would only store information when a specific event occurs and store a record of that as a transaction. The transaction is evidence of a specific instance of an event occurring. So, yes data records are never updated or deleted.

Sensitive identifiers are not written to the data store? This is the biggest challenge and all data would be anonymised. The auditors are not interested in the personal details of the SUs, they are only interested the quality of care the SU receives. This issue has been discussed for this application in [12] and all the Caldicott principles are adhered to. So, yes there are no sensitive identifiers written to the blockchain.

Who would control the data? The blockchain would be permissioned and central control be given to the auditing agency, e.g. CQC. So, yes the auditing agency would have control of nodes and therefore the data.

A tamperproof log of all the writes to the data store? This is absolutely necessary to ensure that the medication is administered correctly and therefore, yes a tamperproof log is required.

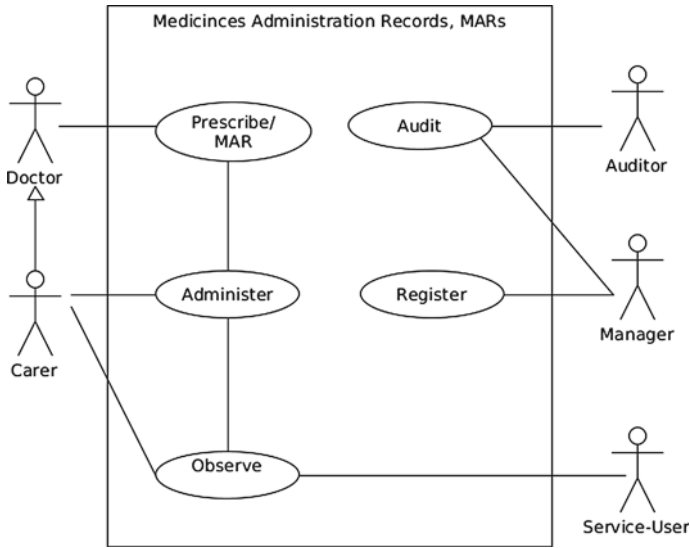


Fig. 1 Use case diagram for medication administration records, MARs

In essence, the above questions have all affirmative answers and therefore Medication Administration Records is conducive to blockchain technology. Any negative answers to the above would require further research and proceed with caution. This stage is probably the most important and decides whether to progress to the following subsections.

3.2 Use Case

Figure 1 illustrates the Use Case Diagram for the system. The use case shows the interaction of participants with the system and each use case is described below:

Register: The registration and deregistration of an SU to an instance of a CHP is completed by a manager. This registration would trigger smart contracts, that may re-order prescriptions from a medical professional and more. Smart contracts would invalidate any further MARs entries and prevent re-ordering of prescriptions to the same Care Home provider when an SU has been deregistered. All transactions are recorded anonymously on the blockchain.

Prescribe: The Doctor participant in our use case diagram is responsible for generating the prescription, which in turn generates the MAR sheet. This procedure may differ from country to country, in the UK the prescription is forwarded to the pharmacy, who dispense the medication and generate the corresponding MARs sheet. A prepared MAR sheet will include the dosages, timings, medicine administer code

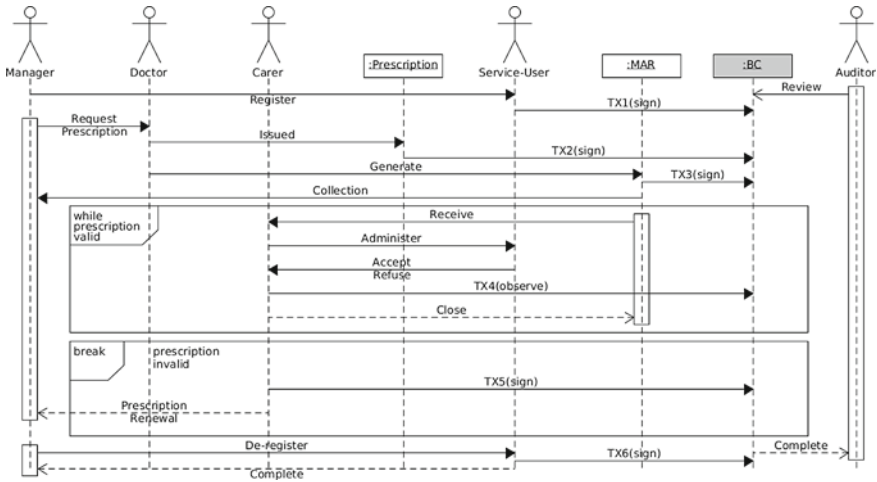


Fig. 2 Sequence diagram for medicine administration records blockchain application

(e.g. oral), and other information for the duration of the prescription, which can be 28 days or 1 week.

Administer: The carer will administer the medication overtly and thus allow the SU to refuse or reject the dosage. This would then be recorded; such actions could involve the smart contract contacting for further medical assistance or advice.

Observe: Any reactions that are abnormal would be recorded and observed and then the Carer would provide further support by looking at the SU’s personal care plan and request further professional advice of how serious the consequences are.

Audit: Auditors can audit the system at any time, as can managers. The Auditors cannot identify individuals from querying the blockchain. Running smart contracts will have sufficient privileges to access generated MARs and determine from the blockchain if any transgressions should be brought to the attention of the Auditor. The system is not concerned with attribution and this would be the responsibility of the Auditing agency and the Manager.

Once agreed and completed, the modelling moves to the next stage, the sequence diagram. Normally, a class diagram would be produced for data, however, there is probably an adequate database with the information installed and therefore this would not be required. If there is no database then a class diagram would be required, we have skipped this part since the database already existed and the blockchain complements the database, not replaces it.

3.3 Sequence Diagram

The sequence diagram will help identify the transactions explicitly and independently. The traditional approach to sequence diagrams is to have a sequence diagram per use case, however, a holistic approach has been taken and consider the overall system as a sequence diagram and in it identify the transactions.

Figure 2 illustrates the sequence diagram and the key issue in this diagram is the addition of the blockchain, represented by the class BC. This would not appear in the class diagram and at first would appear as an error. This is deliberate and represents the information store on the blockchain. There are *six* different types of transactions (TX) represented in the lifecycle of a MAR sheet, and they are described below:

TX1: is to ensure that an immutable record is kept of the registration of an SU to a care provider by a manager and prevent medication being administered to unregistered SUs. Information included: manager signature, SU primary key, care home primary key and timestamp.

TX2: is to ensure that an immutable record of the prescription by a qualified medical professional. Other systems will record this and it is not the intention of this system to control the ordering and re-ordering of prescriptions. This system is just to record the prescription has been completed. The identity of the individual is kept anonymous and has to be completed before a MAR sheet can be generated. Information included: SU primary key, digital signature of the Doctor/Participant, and timestamp.

TX3: is to ensure that an immutable record of the generation of the MAR sheet. Documents stored on blockchain is frowned upon, since they would require constant updates and contradict one of the questions on never changing information, so it is not the MARs sheet that is stored on the blockchain, but a record of it being generated. Information included: SU primary key, digital signature of the generator and timestamp.

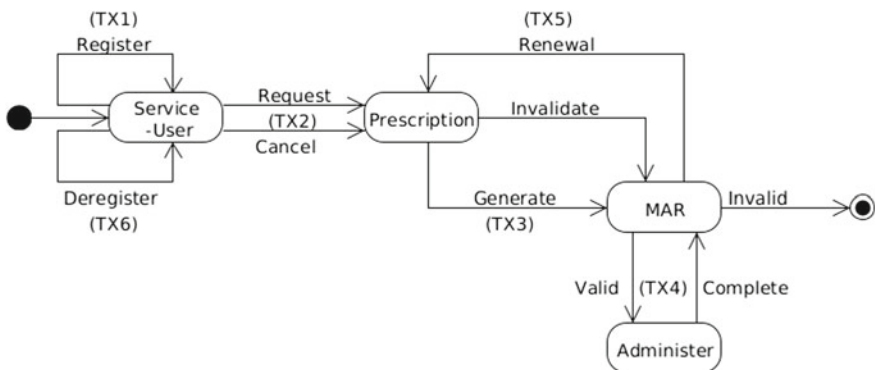


Fig. 3 State machine diagram for medicine administration records blockchain application

TX4: is to ensure that an immutable record of the administration of a medicine to an individual. This record is repetitive and continues until the prescription becomes invalid. It would include: carer signature; SU primary key; MARS primary key; timestamp; and, observation notes.

TX5: is to ensure that an immutable record is kept of when the prescription becomes invalid and a renewal process is requested. Essentially, this is when the MARs sheet runs out of rows to complete and a new one is reordered, however, there could be other reasons, e.g., patient is showing a bad reaction to medication. This also ends the combined fragment in Fig. 3. Information included: carer signature, SU primary key and timestamp.

TX6: is to ensure that an immutable record is kept of the deregistration of an SU from a home. This would be completed by a manager and invalidate any MARs entries. There would be a period of grace for transition and agreed by the manager and dependent on the SU's needs. Information included: care home primary key, manager signature, SU primary key and timestamp.

The use case, along with knowledge of the MARs procedure has informed the identification of the transactions above. The next stage is to think of each of these transactions and what further events they can trigger. The next section considers smart contracts modelling with state machine diagrams.

3.4 Smart Contracts—State Machine Diagram

In [16] smart contracts, SCs, are defined as, "... business rules and state...". SCs automatically update the ledger when certain pre-conditions are agreed. The design of these has been covered in [17], despite the excellent description and case study, this primarily looked at individual smart contract design and was completed using unorthodox diagrams. Our challenge is to observe the state change for each of the transactions, and there is no better diagram than UMLs state machine diagrams. Figure 3 shows the state machine diagram for the case study and associates each of the transactions, TX1-6, identified in Sect. 3.3.

Then a detailed analysis, much like the one offered in [17], is required of the possible smart contract implications. For example, the smart contracts for the completion of a MARs entry could complete the automatic renewal request when its state is 5 working days, estimated time to renew prescription, from completion. During an audit of this nature it is what is missing, not present, that indicates errors. MARs entries left empty are crucial and indicate the omission and are not to be confused with SU's refusal or inability to accept medicines, of the administering of a prescribed medicine. Again, smart contracts would be responsible for highlighting these omissions to auditors, they could even be used to help prevent omissions due to forgetfulness and remind Healthcare professional of an imminent medicine requiring administering, reduction in omissions have been recorded in [18] as a result of sending reminders to healthcare professionals.

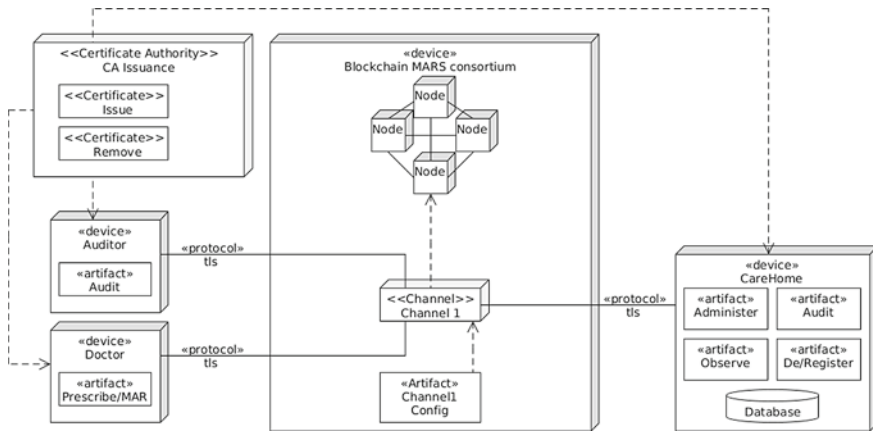


Fig. 4 Deployment diagram for medicine administration records blockchain application

Such detail is crucial to the development of a future Decentralised Autonomous Organisation, DAO. Until now everything is suggest in a sequence, however, the next sub-section can be completed in parallel with the detailed analysis of smart contracts, and concerns the physical architecture.

3.5 Architecture—Deployment Diagram

Figure 4 illustrates the UML deployment diagram. The Blockchain MARs consortium would be deployed on the auditing agency’s server, in the UK this is the CQC. For auditing networks, the control is normally centralised to a governing body that can be trusted. Within this device access to several ‘Nodes’ or ‘peers’ is permitted, which are used to determine, via consensus, the blocks added to the blockchain. Each node would have its own copy of the blockchain, which would be accessible for querying for Audits.

Note that the CHP has its own database, and that the proposed blockchain system is not to replace the database, but complement it by providing an append-only ledger that is updated by secure protocol and can be used for auditing purposes. Such a database that could be reflected in the class diagram model for data and provide key information as to the attributes being passed.

The auditor would not have system access, but would be granted read access privileges by. Certificate authorities would issue various certificates to communicate and would be part of the channel configuration.

Normally, instances on a deployment diagram are not shown, however, it is important to consider the consequence of adding another instance of a CHP. In our case study, the instances of Doctor and Auditor have no consequence to the physical design. However, the introduction of a second CHP has a significant effect. This is

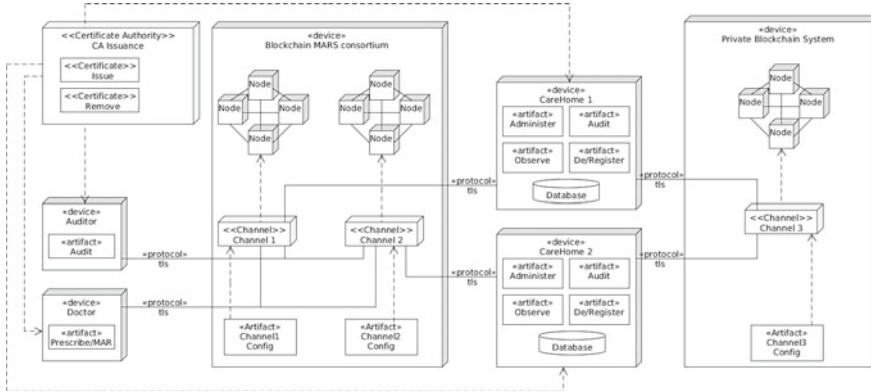


Fig. 5 Deployment diagram for multi-channel architecture for medicine administration records blockchain application with two Care Home Providers (CHP)

something worthwhile considering during the design stage, to determine if a single channel is sufficient for communication as the number of instances increase. This is discussed in the next sub-section.

Multi-Channel Fig. 5 shows two organisations, CHP 1 & 2. These devices represent managers and healthcare professionals, essentially all devices working in the Care Homes under a single organisation. GDPR [19] and National data protection laws, see [20], permits sharing data within an organisation and therefore multiple care homes managed by a single organisation operate under a single channel. Naturally, there would be restrictions in place to prevent unauthorised access and this can be completed using ABAC [21], that is supported by Hyperledger.

This does require access by both Doctors and Auditors, so use cases for auditing and prescribing/MARs would have to reflect the correct channel and certificate to use - this would probably require a portal to access the individual CHPs.

The separation of a group of nodes indicate that there are two ledgers, one for each channel. Access control can be implemented to restrict access to only trans-actions from a particular care home. Therefore, there is a decision to implement a multi-channel blockchain, each channel having its own ledger. Terminating blockchains can also be difficult and the ledgers could easily be removed and would not persist elsewhere by closing the channel and therefore removing the associated nodes, e.g., where a CHP fails accreditation and is removed.

Throughput is difficult to estimate, however the blockchain system can be optimised based on: blocksize; number of channels; StateDB used; and, peer resources. Optimising these for your Hyperledger consortium is discussed in [22] and should be considered when designing your architecture. Depending on the settings [22] shows that these can exceed 2000 transaction per second (TPS) for a single channel network.

Finally, something outside the realms of this paper, there is the opportunity for the two CHPs to communicate via their own private blockchain. This could be the hiring of staff, use of temporary staff or other resources these organisations may share.

4 Evaluation

The prototype was built using hyperledger composer [23]. Whilst deprecated, it is an excellent tool for building prototype permissioned blockchains before the construction on hyperledger fabric.

One issue that was soon apparent is that people make mistakes, or user errors. This did not stop the model, nor information being stored on a blockchain. It is not unusual for someone to push or click a wrong button on a form, whilst this would still be recorded on the blockchain, an additional functionality was added to include the reversal of this action and another TX. This would be followed by the corrected action and an appropriate TX made—users should be made aware that mistakes cannot be altered, only corrected and this does not overwrite the error, merely adds a new block demonstrating that the previous error is acknowledged and a further transaction is to be made to make the appropriate correction. This correction facility is time-bound and cannot be completed after a certain time has elapse from the original submission.

In summary, here there are five important stages of development for blockchain engineering:

1. **Blockchain Efficacy Analysis:** Is the dog wagging the tail, or the tail wagging the dog. Is blockchain generating problems, or being used to solve them? Is the blockchain system proposed the most effective technology to provide a solution to the given problem. Auditability is conducive to blockchain, but it does not mean every audit requires a blockchain.
2. **Use Case:** Identify the main updates required for the blockchain.
3. **Sequence Diagram:** Identify the key transactions to generate information on the blocks.
4. **Smart Contracts:** Use state machine diagrams to model state changes, these should help identify the transactions and where smart contracts can interact with the system.
5. **Deployment:** Most permissioned blockchains are going to have a similar deployment figure. You need to identify the use cases and how and where they are deployed.

The modelling of blockchain certainly helped with the design, but more with maintenance and explanations. Explaining with the aid of diagrams is always going to be easier than explaining code. The BMARs was implemented with success and exists as a prototype blockchain consortium, further results can be found in [1].

5 Conclusion

The main contribution is twofold: (i) application of decentralised systems to health-care; and, (ii) a *five* stage to modelling process for blockchain applications. Specifically, this model was applied to an auditing network and may not adapt so easily to

a different type of network, e.g., a supply-chain. In such cases different models may be used, such as BPMN, to accommodate the change in the blockchain application, see [24] for further information.

This offers a template for the design of a blockchain consortium for auditing. There may be differences between auditing services, but in general there are going to be several crucial decisions, that will revolve around the architecture and type of throughput required. If the throughput is high, say $\gg 1,000$ TPS, then optimisation of the network will need to be considered, this could be a single channel, or smaller blocks. If the throughput is low, say < 100 TPS, then you can afford to have more peers and a greater number of channel without little consequence to the latency of each block submitted.

There is a long way to go in modelling blockchain. At the time of writing the technology supporting blockchain is [4] *twelve* years old. There have been many major developments, from Ethereum to Hyperledger, but there is a need for a common method to model blockchains and this *five* stage methodology is making a start.

Acknowledgements Author would like to thank Dr Harjinder Rahn for consultation during the development of this paper and the reviewers for their feedback and general comments.

Competing Interests None identified.

References

1. Mitchell I, Hara S (2019) BMAR—blockchain for medication administration records. *Blockchain and Clinical Trial—Securing Patient Data*, pp 231–248
2. Cabatic GV (2018) 159 AD3d 62. New York, Supreme Court, App. Div, 2nd Dept
3. Justard J (2020) Filling out medication administration records. <https://dphhs.mt.gov/Portals/85/dsd/documents/DDP/MedicalDirector/MARs-howtofillthemout.pdf>. Accessed Aug 2020
4. Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system
5. Castro Miguel, Liskov Barbara et al (1999) Practical byzantine fault tolerance. OSDI 99:173–186
6. Lamport L, Shostak R, Pease M (1982) The byzantine generals problem. *ACM Trans Program Lang Syst (TOPLAS)* 4(3):382–401
7. National Institute for Health and Care Excellence. *Managing medicines in care homes*, March 2014. nice.uk.org/guidance/sc1
8. Azaria A, Ekblaw A, Vieira T, Lippman A (2016) Medrec: using blockchain for medical data access and permission management. In: *Open and big data (OBD)*, international conference on. IEEE, pp 25–30
9. Kumar R, Tripathi R (2019) Traceability of counterfeit medicine supply chain through blockchain. In: *2019 11th international conference on communication systems & networks (COMSNETS)*. IEEE, pp 568–570
10. Vithanwattana N, Mapp G, George C (2017) Developing a comprehensive information security framework for mhealth: a detailed analysis. *J Reliable Intell Environ* 3(1):21–39
11. Caldicott F (2013) *Information: to share or not to share? The information governance review*. Dept. of Health, UK
12. Mitchell I, Hara S (2019) Quality audits and blockchain for healthcare in the uk. In: *Health IT workshop (HITWS)*

13. Wood G (2020) Web 3.0 foundation. web3.foundation. Accessed: Aug 2020
14. Yaga D, Mell P, Roby N, Scarfone K (2018) Blockchain technology overview. Technical report, National Institute of Standards and Technology
15. Oscar Research Ltd (2020) Care homes in the uk. <https://www.oscar-research.co.uk/datasheets/carehomes>. Accessed Aug 2020
16. Bashir I (2018) Mastering blockchain. Packt, 2 edn
17. Karamitsos I, Papadaki M, Al Barghuthi NB (2018) Design of the blockchain smart contract: A use case for real estate. *J Inform Secur* 9(3):177–190
18. Bennett JW, Glasziou PP (2003) Computerised reminders and feedback in medication management: a systematic review of randomised controlled trials. *Med J Aust* 178(5):217–222
19. Council of European Union. Council regulation (EU) no 2016/679. <https://eur-lex.europa.eu/legal-content/en/LSU/?uri=CELEX%3A32016R0679>. Accessed Aug 2020
20. Carey P (2018) Data protection: a practical guide to UK and EU law. Oxford University Press, Inc.
21. Hu VC, Ferraiolo D, Kuhn R, Schitzer A, Sandlin K, Miller R, Scarfone K (2014) Guide to attribute based access control (ABAC) definition and considerations. SP 800-162
22. Thakkar P, Nathan S, Vishwanathan B (2018) Performance benchmarking and optimizing hyperledger fabric blockchain platform. arXiv preprint [arXiv:1805.11390](https://arxiv.org/abs/1805.11390)
23. Gaur N, Desrosiers L, Novotny P, Ramakrishna V, O'Dowd A, Baset SA (2018) Hands-on blockchain with hyperledger: building decentralised applications with hyperledger fabric and composer. Packt
24. Weber I, Xu X, Riveret R, Governatori G, Ponomarev A, Mendling J (2016) Untrusted business process monitoring and execution using blockchain. In: International conference on business process management. Springer, pp 329–347