International Journal of Artificial Intelligence and EvolveTech
ISSN: 0000-0000
Volume 1, Issue 1 | PP 1-8 | www.ijaiet.com |

Blockchain-Enabled Data Integrity in Distributed Healthcare Systems: A Taxonomy of Consensus Mechanisms and Applications

Dr Neelam Goyal

Dean - Behavioural Sciences, Sardar Patel University, Sikkim

*Corresponding author
Dr Neelam Goyal
Dean - Behavioural Sciences, Sardar Patel University, Sikkim https://www.spusikkim.edu.in Email:
dr.neelamgoyal15@gmail.com

Received : 25-06-2026 | Revised :10-08-2026 | Accepted : 25-08-2026 | Published : 31-08-2026

Abstract

Many of the organisations that produce, store and share healthcare information including hospitals, labs, pharmacies, insurers and device manufacturers are all distrustful of one another, and their ability to ensure the integrity of the data, its resistance to unauthorised alteration, and its verifiable provenance is challenging to guarantee across such fractured systems. The distributed ledger technology known as blockchain cryptographically linked blocks of records that make it difficult to tamper with or alter data is one possible candidate for the infrastructure to support this assurance of data integrity without a central trusted authority. The consensus mechanism is the protocol used to agree on the content of the ledger between distrustful nodes, and its impact on a system's throughput, latency, energy usage, fault tolerance and decentralisation determines its suitability for clinical applications. This paper presents a survey of the existing consensus mechanisms and proposes a healthcare-oriented taxonomy of consensus mechanisms. It defines the work in four directions: taxonomy of consensus families, proof-based, stake-based, voting/Byzantine-fault-tolerant and hybrid consensus families; comparative analysis of their performance, security and decentralisation trade-offs with the blockchain trilemma; mapping healthcare applications onto consensus and permission families (electronic health record sharing, consent management, pharmaceutical supply-chain provenance, clinical trials, and remote monitoring); and open challenges of privacy versus transparency, scalability, regulatory compliance and interoperability. The survey shows that deployments in the healthcare sector are dominated by permissioned, voting-based systems like proof-of-authority and practical Byzantine fault tolerance, which have a higher transaction throughput, faster finality, and low energy cost that fulfil the clinical requirements, compared to energy-intensive proof-of-work. The most important design principle is to match up the consensus mechanism to the level of integrity needed for each application rather than using a single ledger for them all.

Keywords: blockchain; data integrity; distributed healthcare systems; consensus mechanisms; electronic health records; distributed ledger technology; Byzantine fault tolerance

1.Introduction

Healthcare is a distributed business these days. One patient's data is created and updated in multiple hospitals, clinics, labs, drug manufacturers, and increasingly, personal and implanted medical devices, none of which is fully trusted by the others and all of which must share data to provide care. In this environment, data integrity is key and difficult to ensure because data can be modified without permission and its source and history can be traced. Centralised databases mean that integrity is in the hands of one entity and there is one point of failure and compromise the case

of federated arrangements, which struggle to provide a shared, tamper-evident audit trail across organisational boundaries [1].

Blockchain technology provides an alternative way of establishing trust. A blockchain is a distributed database of transactions, cryptographically hash-linked and appending to the new ones; once a record is made to a blockchain, it cannot be altered without requiring the reconstruction of all future transactions on the blockchain by the majority of independent nodes. The result is tamper-resistant and verifiable provenance without a central authority, which naturally fits into the need for trustworthy records in healthcare which are shared among distrustful parties [2], [3]. The literature on blockchain applications in electronic health record (EHR) sharing, consent management, pharmaceutical supply chains, clinical trials, and device data integrity [4] has been expanding over the years.

The feature that makes a blockchain so trustworthy and that most clearly restricts the practical applications of it and its nodes is its consensus process: the protocol by which independent nodes agree on which transactions are valid and accepted and in what order, even when failures or adversaries occur. The throughput, latency and finality, energy consumption, fault tolerance and decentralisation of a blockchain are all influenced by the consensus mechanism, and these qualities are mutually exclusive, which is known as the blockchain trilemma: security, scalability, and decentralisation [5], [6]. Clinical workflows demand high throughput, rapid finality, cannot be easily scaled with the energy consumption of proof of work, and have to comply with strict regulatory and privacy requirements in healthcare. This makes the selection of consensus mechanism an important but not insignificant consideration when deciding whether a blockchain can be used clinically.

Based on the consensus perspective, this paper reviews the concept of blockchain-based data integrity in distributed healthcare. It aims to answer four questions: (RQ1): What consensus mechanisms are there and how can they be organised in a taxonomy? (RQ2): How are performance, security and decentralisation balanced? (RQ3): What are the applications of blockchain in healthcare with data integrity problems and which consensus and permission model is suitable for them? (RQ4): What challenges are there to address? It provides a taxonomy of consensus mechanisms (Figure 1), a comparison of mechanisms and their trade-offs (Table 3), a layered reference architecture that maps applications onto the mechanisms (Figure 2, Table 4), and open challenges and design guidance (see Table 6).

1. Review Approach

1.1 **Method.** This is an organized survey of the narrative with a predetermined protocol which included the research questions, the literature sources, the inclusion criteria, and the extraction and synthesis process prior to the screening process. The field, distributed-systems theory, cryptography, and health informatics, and the incommensurable outcomes of the field, are better suited to a narrative than a meta-analytic synthesis.

1.2 **Scope and eligibility.** The survey includes work on using blockchain or distributed-ledger technology for data integrity, provenance, or security in a healthcare setting that explicitly or implicitly involves a consensus or permission model. Generic cryptocurrency and finance applications and healthcare-IT applications (without ledger dimension) are out of scope. All criteria are listed in Table 1.

1.3 **Information sources and search strategy.** The clinical-informatics literature was supplemented by citation chasing and scanned in five databases: IEEE Xplore, the ACM Digital Library, Scopus, Web of Science, and PubMed. The search was done in combination with three concept blocks (blockchain, data integrity and security, and the healthcare setting) and Boolean operators that were modified to fit each database, as shown in Table 2.

1.4 **Selection and extraction.** Records retrieved were de-duplicated, screened by title and abstract and by full text (the number retained after each screening should be noted in the final manuscript) against eligibility criteria. A general template was developed for each of the works they retained, and the consensus mechanism, permission model, healthcare application, targeted property of the integrity, and the reported performance or evaluation were recorded.

2.5 Synthesis. The results were presented in a thematic format according to the four research questions. Consensus mechanisms were aggregated into the taxonomy of Figure 1, compared in Table 3, and then embedded in the stack of a healthcare system in the reference architecture of Figure 2, with applications mapped to the consensus models (and permission models) that are suitable for them in Table 4.

Table 1. *Scope and eligibility criteria for the survey.*

Dimension	Inclusion criteria	Exclusion criteria
Focus	Blockchain / DLT applied to integrity, provenance, or security in healthcare	Generic cryptocurrency/finance; no integrity dimension
Setting	Distributed healthcare systems (EHR, IoMT, supply chain, trials)	Non-health domains
Contribution	Architecture, consensus mechanism, application, or review	Non-technical opinion pieces
Type	Peer-reviewed papers and well-cited preprints	Non-archival abstracts and posters
Language	Published in English	Full text unavailable in English
Window	Modern blockchain-in-health era (2016–present)	Pre-dates the relevant literature

Table 2. *Search concept blocks and representative terms; syntax was adapted to each database.*

Concept block	Representative search terms (OR-combined within block; blocks AND-combined)
A · Blockchain	blockchain OR "distributed ledger" OR DLT OR "smart contract" OR consensus
B · Integrity & security	"data integrity" OR provenance OR tamper OR immutab* OR auditability OR security OR privacy
C · Healthcare	healthcare OR "electronic health record" OR EHR OR clinical OR medical OR IoMT OR "health data"
D · Consensus (optional)	"proof of work" OR "proof of stake" OR PBFT OR "proof of authority" OR Byzantine

3. Findings

3.1 Blockchain and data integrity in healthcare. The three properties combine to give a blockchain integrity. Cryptographic hash-linking makes each block depend on the previous one, so that tampering is easily detected; each node is independent and will not fail if the other fails; and consensus will allow honest nodes to settle on one agreed-upon history. Another important architectural attribute when it comes to healthcare is whether the ledger is permissionless, meaning open and accessible to anyone, like in public blockchains, or permissioned, where access is limited to certain entities, as in a consortium of hospitals [7]. Clinical data is sensitive, and the entities that hold it are known, which has led most healthcare deployments to either permissioned or consortium ledgers, and, typically, only hashes or pointers on-chain, with relevant bulk records stored off-chain, to allow for data minimisation and respect for privacy [8]. The four research questions addressed below are framed in this background.

In healthcare, threats to integrity are real, including unauthorized changes to patient records, which could mask errors or fraud; the loss of a clear audit trail between departments or organizations, which would lose a verifiable record of patient care interactions; the introduction of fake products or falsified patient readings into the clinical workflow; and unauthorized access and manipulation of patient data. Any change to a committed record is immediately apparent on a blockchain and the blockchain itself serves as an immutable audit trail and attaches provenance from one custodian to another in the third. It's crucial, however, to understand the limits of the guarantee: while blockchain can guarantee that what was written on the ledger is correct, it cannot guarantee that the information entered is correct. Integrity of the ledger is ensured, but it is important to pair this with proper data entry validation and identity management protocols to realize clinical meaning of the data stored on the ledger, as misinformation or malicious information entered by an authorised user is also preserved as faithfully.

3.2 RQ1 A taxonomy of consensus mechanisms. In Figure 1, consensus mechanisms can be found in four families. Proof-based mechanisms force participants to use a resource that is limited, such as proof-of-work (PoW), the original

Nakamoto consensus, but other mechanisms, proof-of-elapsed-time (PoET) and proof-of-capacity (PoC), rely on trusted timers or storage [9]. Using stake-based mechanisms instead of physical work, economic stake proof-of-stake (PoS) and delegated proof-of-stake (DPoS) choose block proposers based on the value staked, reducing energy costs. Voting- or Byzantine-fault-tolerant (BFT) mechanisms are based on classical distributed-systems theory: Practical Byzantine fault tolerance (PBFT) which aims for consensus among a known set of nodes with up to one-third of malicious nodes [10]; and proof-of-authority (PoA), which depends on a small, vetted group of validators and crash-tolerant protocols like Raft, which assume non-malicious failures only. These ideas or the rejection of the linear chain are the basis of hybrid schemes or schemes based on the DAG. The mechanisms within each family, and this organisation, are summarised in Figure 1 and compared in detail in Section 3.3 [5], [11].

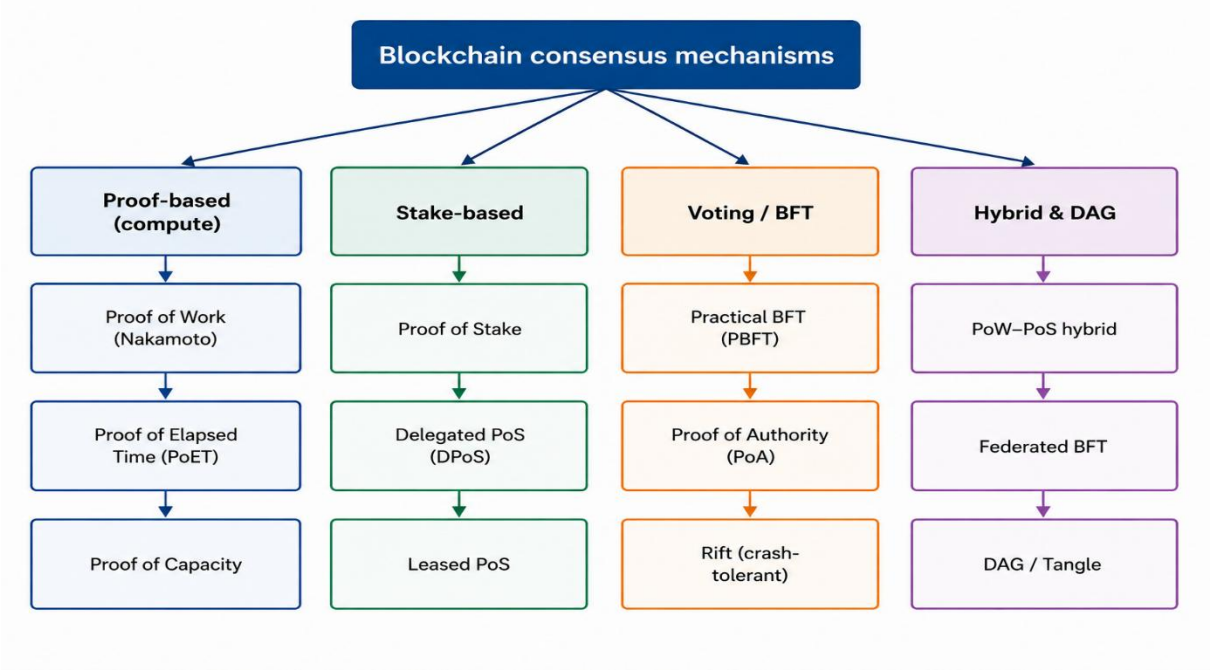

Figure 1. *A taxonomy of blockchain consensus mechanisms relevant to distributed healthcare systems.*

3.3 RQ2 Comparative trade-offs. The families have opposing views about the size of the healthcare dimensions as shown in Table 3. PoW is well-suited for open, permissionless environments, but has very high energy consumption, low throughput, and only probabilistic finality properties, which are unfit to clinical workflows at scale [12]. PoS and DPoS have the benefit of openness and reduced energy consumption and increased throughput but have stake-centralisation issues. The BFT family is the obvious choice for permissioned healthcare consortia: PBFT and PoA offer high throughput, finality and low energy cost – though with the downside of needing to scale to only moderate validator numbers and have their identities known [13]. The crash-tolerant protocols like Raft are more performant, but can only handle benign failures, not malicious ones, and are appropriate for highly trusted deployments. There's no solution that optimises all three aspects simultaneously, as there's a tradeoff between scalability, performance, or decentralisation, or between decentralisation and trust assumption. The take-home lesson is that selecting a mechanism is a step that has to be taken after considering the specific integrity, performance and trust requirements for the application.

Table 3. *Comparative taxonomy of consensus mechanisms against dimensions relevant to distributed healthcare.*

Mechanism	Family	Permission model	Fault tolerance	Throughput	Energy	Healthcare fit
Proof of Work	Proof-based	Permissionless	≤50% honest hash	Low	Very high	Poor (energy, latency)

International Journal of Artificial Intelligence and EvolveTech
ISSN: 0000-0000
Volume 1, Issue 1 | PP 1-8 | www.ijaiet.com |

Mechanism	Family	Permission model	Fault tolerance	Throughput	Energy	Healthcare fit
Proof of Stake	Stake-based	Both	≤50% stake	Medium	Low	Moderate
Delegated PoS	Stake-based	Both	Delegate-based	High	Low	Moderate
PBFT	Voting / BFT	Permissioned	≤⅓ Byzantine	High	Low	Strong (consortium)
Proof of Authority	Voting / BFT	Permissioned	Authority-based	High	Very low	Strong (consortium)
Raft	Crash-tolerant	Permissioned	Crash only	High	Very low	Good (trusted nodes)
Hybrid / DAG	Hybrid	Varies	Varies	High	Low	Emerging

3.4 RQ3 Applications and a reference architecture. Blockchain data-integrity systems for health care can be broken down into the layers of Figure 2. The clinical use cases are located in an application layer, while the smart-contract layer contains access policies, provenance rules and audit logic. The consensus layer provides agreement that remains tamper evident, the network and ledger layer has the replicated, hash linked chain, and the off-chain storage layer contains bulk clinical data, which is referenced by on-chain hashes. Cutting across the stack are the requirements of integrity, privacy, auditability, interoperability, and regulatory compliance. In this structure, the different applications have different requirements for consensus as presented in Table 4. EHR sharing and consent management focus on tamper evident records and immutable access trails, with permissioned PBFT or PoA [14]–[16] being preferred. Next, there is the need for end-to-end custody provenance, over a consortium, for pharmaceutical supply-chain and anti-counterfeiting systems, which is also well met by BFT-type agreement. The clinical-trial systems should include tamper-proof audit trails for regulatory auditing, the remote patient monitoring over the IoMT should involve low latency and lightweight validation of high frequent device data, favouring efficient PoA or hybrid schemes [17], [18]. Interoperability designs focus on the design of the ledger to be aligned with the health data standards that allow for verifiable cross-organizational exchange [19].

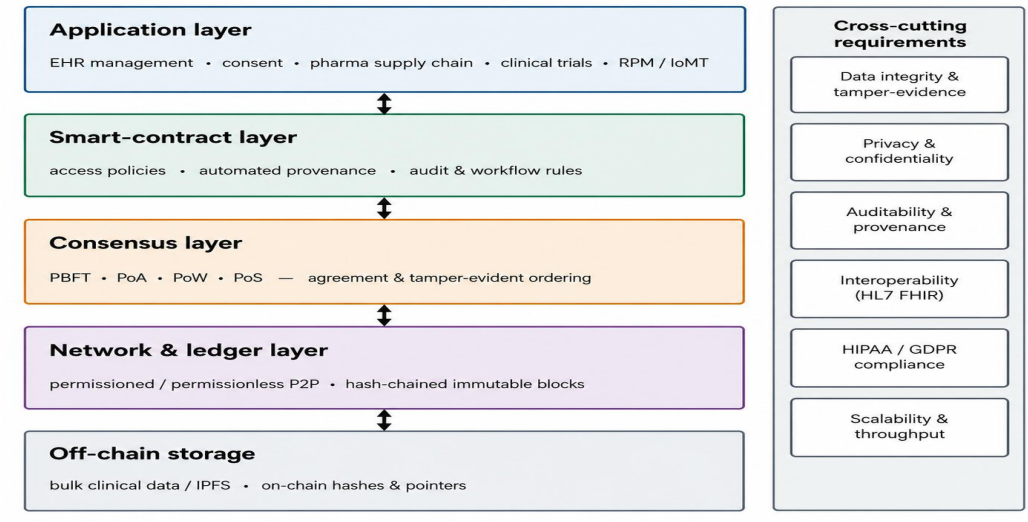

Figure 2. *A layered reference architecture for blockchain-enabled data integrity in distributed healthcare systems.*

Table 4. *Healthcare applications mapped to their integrity role and suitable consensus and permission models.*

Application	Integrity role	Typical on-chain data	Suitable consensus / model
EHR management & sharing	Tamper-evident records; access audit trail	Record hashes; access events	Permissioned PBFT / PoA
Consent & access management	Immutable, verifiable consent history	Consent events; policies	Permissioned PoA / PBFT
Pharma supply chain	End-to-end custody provenance	Custody events; serials	Consortium PBFT / PoA
Clinical trials	Tamper-proof audit of protocol & results	Timestamps; result hashes	Permissioned PBFT
Remote monitoring (IoMT)	Integrity of device data streams	Sensor-reading hashes	Lightweight PoA / hybrid
Health data exchange	Verifiable cross-organizational sharing	Standardised references; pointers	Consortium PBFT / PoA

3.5 RQ4 Open challenges. The following four challenges are repeated in the literature. The dilemma of privacy versus transparency: On-chain log storage usually contains hashes and pointers, and not the sensitive content, because sensitive information needs privacy while the ledger needs transparency as it is tamper evident [18]. Scalability: Although efficient permissioned systems can be designed, as networks and data increase, there are throughput and storage constraints which push for the development of off-chain channels and sharding [6]. Data-protection rights: There is a tension between immutability and data-protection rights, like rectification and erasure, as architectural decisions about what is committed to the chain must be made. [20] Interoperability: Achieving mutual benefit requires linking ledgers to health data standards and governance mechanisms between the institutions involved [19]. These are the main hurdles that must be overcome to make it from promising prototypes to production clinical systems.

4. Discussion

4.1 Principal findings. Three conclusions emerge. The consensus mechanism is the most important design feature that governs the trade-offs between throughput, finality, energy, fault tolerance and decentralisation that are essential to viability in healthcare. Second, that trade-off always works one way for most healthcare scenarios: for known, regulated organisations where the high throughput and ability to confirm transactions immediately outweigh open participation of candidates without permission and where energy-intensive PoW is largely disqualifying, the trade-off works one way: that is, towards PBFT or PoA. Third, there is no universal ledger, every application has its own integrity need so mechanism to use case is the guiding rule, do not standardise on one chain.

4.2 Matching consensus to healthcare requirements. The comparison and mapping of application helps to find a simple design heuristic. Crash-tolerant protocols optimise performance when participants are limited and trusted; when the participants are a known but not fully trusted consortium, a Byzantine-fault-tolerant (BFT) protocol like PBFT or PoA offers the best balance of integrity, performance and moderate energy cost; and only when open, permissionless participation is truly needed, is it desirable to look at stake-based mechanisms, where PoW would be used in settings where maximal decentralisation is valued over efficiency. This selection is often used in combination with an off-chain storage strategy where only hashes that guarantee data block integrity are stored on the ledger [8].

4.3 Implications for practice. The taxonomy and reference architecture presented a daunting design space to system designers, as it involves a series of choices: selecting a permission model based on the trust relationships between the participants, selecting a consensus family based on the trust relationships and the required fault conditions and performance, and determining what should be on-chain versus off-chain based on privacy and regulatory considerations. For healthcare organizations, the analysis also shifts the discussion from a technical one to a governance one; with a permissioned consortium, member organizations must agree on who will be the validators, on the standards that will be used for data, and on how to handle erasure and rectification rights.

4.4 When blockchain is and is not warranted. The analysis also sheds light on when a blockchain is not the appropriate tool. Availability: If a single trusted custodian is sufficient, and inter-organisational validation is not needed, a well-governed centralised database, which has robust access controls and cryptographic audit logging, can provide similar integrity at a reduced complexity and cost. Blockchain gets its overhead where integrity needs to be maintained between a series of parties that aren't necessarily 100% trusted, and when there's a need for a shared, tamper-evident record. Awareness of this boundary helps prevent implementing distributed ledgers in situations in which their unique characteristics are never put into practice, as is often the case in the early pilots of healthcare distributed ledgers.

4.5 Limitations of this survey. This review is a narrative synthesis and represents editorial selection and organization of a large and rapidly evolving literature, and was limited to English-language publications from the modern era of blockchain-in-health research. The taxonomy and reference architecture are analytical scaffolds that help to organize the field and not a complete enumeration; performance results reported in the primary literature, if they are results, are often acquired in non-standard conditions in which a direct comparison can be made. The following restrictions should be clearly mentioned in the final manuscript.

5. Conclusion

Ensuring the security and trustworthiness of health information in a distributed, distrustful environment is an old issue that blockchain can provide a unique solution: Immutable, verifiable records that do not require a trusted third party. This survey has claimed that the consensus mechanism is the key that unlocks the clinical viability of such systems, and has categorized the field into proof-based, stake-based, voting/BFT and hybrid mechanisms and done a comparative analysis of the trade-offs between the different mechanisms and the blockchain trilemma, presented a layered reference architecture to map appropriate consensus and permission models to healthcare applications, and presented an analysis of the remaining challenges of privacy and scalability, regulatory concerns and interoperability. The recurring theme is that the Byzantine-fault-tolerant approach is the one that works best in the known-participant, high-throughput, energy-constrained reality of healthcare; and that the design of a mechanism is the correct one for it to match the integrity requirements of a given application, not a single ledger for everyone. Achieving the promise at scale requires not just more in the way of advances in consensus, but also the right governance, standards, and regulatory alignment.

Declarations

Conflict of Interest

The authors have no conflicts of interest to declare.

Funding Statement

The research was not funded with a specific grant from any public, commercial or not-for-profit grant-giving entity.

Ethical Approval

No human or animal subjects were used in this study and ethical approval was not required.

References

[1] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications,” *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017, doi: 10.1093/jamia/ocx068.

[2] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, “Blockchain technology in healthcare: A systematic review,” *Healthcare*, vol. 7, no. 2, Art. no. 56, 2019, doi: 10.3390/healthcare7020056.

[3] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, “A systematic review of the use of blockchain in healthcare,” *Symmetry*, vol. 10, no. 10, Art. no. 470, 2018, doi: 10.3390/sym10100470.

[4] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, “Blockchain in healthcare applications: Research challenges and opportunities,” *Journal of Network and Computer Applications*, vol. 135, pp. 62–75, 2019, doi: 10.1016/j.jnca.2019.02.027.

[5] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020, doi: 10.1109/COMST.2020.2969706.

[6] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018, doi: 10.1504/IJWGS.2018.095647.

[7] E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*, Art. no. 30, ACM, 2018, doi: 10.1145/3190508.3190538.

[8] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying blockchain to securely and scalably share clinical data," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 267–278, 2018, doi: 10.1016/j.csbj.2018.07.004.

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[10] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI)*, pp. 173–186, USENIX, 1999.

[11] W. Wang et al., "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019, doi: 10.1109/ACCESS.2019.2896108.

[12] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Open Problems in Network Security (iNetSeC 2015)*, pp. 112–125, Springer, 2016, doi: 10.1007/978-3-319-39028-4_9.

[13] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Systems with Applications*, vol. 154, Art. no. 113385, 2020, doi: 10.1016/j.eswa.2020.113385.

[14] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *2016 2nd International Conference on Open and Big Data (OBD)*, pp. 25–30, IEEE, 2016, doi: 10.1109/OBD.2016.11.

[15] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based e-health systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019, doi: 10.1109/ACCESS.2019.2917555.

[16] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *Journal of Information Security and Applications*, vol. 50, Art. no. 102407, 2020, doi: 10.1016/j.jisa.2019.102407.

[17] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of Medical Systems*, vol. 42, no. 7, Art. no. 130, 2018, doi: 10.1007/s10916-018-0982-x.

[18] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, Art. no. 326, 2019, doi: 10.3390/s19020326.

[19] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 224–230, 2018, doi: 10.1016/j.csbj.2018.06.003.

[20] T. K. Mackey et al., "Fit-for-purpose?" Challenges and opportunities for applications of blockchain technology in the future of healthcare," *BMC Medicine*, vol. 17, Art. no. 68, 2019, doi: 10.1186/s12916-019-1296-7.