Blockchain Digital Health care use cases

By K. Nagarathna , M.C. Arallimard

Dept. of Electronics and Communication Enineering , Basaveshwar Engineering College, Bagalkot , Karnataka , India

**Abstract:**

Blockchain is a powerful technology for enabling secure data sharing and access between multiple parties. This is a major challenge in digital health, where the privacy and security of medical data is paramount, but where improving the quality of care cannot happen without more coordination in management of patient data across the healthcare system and the ability to apply analytics to population level medical data. In short, blockchain can help digital health by making it easier to share data securely, with patient consent, across very fragmented healthcare systems.

Keywords: blockchain, security, cyberattacks

**Introduction**

One of the biggest challenges around blockchain is distinguishing between the real blockchain-based applications and the hype. This is hard to do because there are still only a few large-scale, real-world implementations of blockchain beyond Bitcoin.

Blockchain’s most revolutionary proposition, delivered through a carefully balanced mix of very advanced cryptography and in-built incentives (in the form of Bitcoin or other crypto-tokens), is that it removes the need for a centrally controlling authority and instead distributes

power across all participants within the blockchain ecosystem. So in theory it can remove the need for a third-party to manage transactions between two entities that don’t know or trust each other digitally, securely and impartially. This works pretty well in the Bitcoin ecosystem, but is still being proven in more traditional business environments.

One of the key benefits of a decentralised system is that end-users – especially consumers, but enterprises, too – would have much more transparency and control over how their data is used. So one of the long term goals of disruptive blockchain-enabled companies is to decentralise the data economy, reclaiming power from Google, Facebook, Amazon and other companies that centralise large datasets for competitive benefit, and instead putting control over how personal and proprietary data is used into the hands of individuals and organisations.

On top of giving end-users more visibility and control over their data, blockchain’s inbuilt payment mechanisms could also enable them to sell it in exchange for crypto-tokens. To make all of this work efficiently and autonomously, AI is applied on top of the blockchain tracking ledger to curate valuable data sets and match sellers with buyers. (See [Fetch.ai](https://fetch.ai/) as an example of a start-up working on a system like this.)

This idea remains more theoretical than reality and could take a decade or more to materialise, if ever. However, over the last few years blockchain has been plugging away at its early growing pains – including bad user interfaces, scalability issues, and the need for greater privacy to protect enterprise IP – and has been proven to solve real but far more specific issues around data reliability and accessibility[2].

**Blockchain Functioning**

• Tracking / registry: Recording information and data in an immutable and transparent way, whereby no party has asymmetric power over the data[3]   
• Data access / transfer: Easing transfer of data between multiple parties, to create a common source of “truth”  
• Identity / authentication: Managing identities and permissions for authentication or verification, including the ability to verify identity attributes without divulging sensitive information  
• Settlements: Revenue settlement by recording movement of goods/revenues or use of services/assets  
• Transactions: Enabling (real-time) payments and transactions  
• Token exchange: Virtual currency/tokens with intrinsic value traded between multiple parties. Virtual currencies can also be pegged to fiat currencies, with equivalent values held in escrow accounts.

## Business benefits of these capabilities

• Security: Blockchain is verified through a consensus system and stored across many nodes, making DDoS(Distributed Denial of Service) cyberattacks and tampering with records extremely difficult  
• Cost efficiency: Middlemen who take a cut of transactions can be removed because consensus mechanisms create trust through transparency  
• Traceability: An immutable record of all transactions can reduce fraud and protect againstliability  
• Business process speed: Automated smart contracts can reduce time of transactions because the process no longer requires manualoversight  
• Token value: Digital assets can hold virtual and real-world value, such as when a virtual token is used for a loyalty points programme  
• Confidentiality: Collaboration between organisations can occur without sharing sensitive information, e.g. individual medical records  
• Neutral and equal: No one company or individual owns the blockchain, encouraging trustworthiness and longevity of the system, e.g. if one of the founding parties leaves, the system will continue to work without them

Given the huge challenge healthcare systems are facing around digitising and sharing medical records, and tracking prescription drug and other medical goods

in the supply chain and delivery, it is no surprise that many are trying to improve processes in healthcare by applying blockchain technology.

Meanwhile, adopting many blockchain solutions for healthcare no longer requires deep first-hand expertise with the technology, since most blockchain-based solutions are now offered like any other software-as-a-service.

## Blockchain healthcare use cases in digital health

### Supply chain transparency

A major challenge across the healthcare sector, as in many others, is ensuring the provenance of medical goods to confirm their authenticity. Using a blockchain-based system to track items from the manufacturing point and at each stage through the supply chain enables customers to have full visibility and transparency of the goods they are buying.

This is a top priority for the industry, especially in developing markets where counterfeit prescription medicines cause tens of thousands of deaths annually. It is increasingly important for medical devices, too, which are proliferating quickly with the adoption of more remote health monitoring, and therefore also attracting the interest of bad actors.

[MediLedger](https://www.mediledger.com/solution-protocols) is a leading example of a blockchain protocol that enables companies across the prescription drug supply chain to verify the authenticity of medicines, as well as expiry dates and other important information.

Key benefits of blockchain (paired with AI):

* Customer confidence: Ability for the customer to track each package’s end-to-end provenance, with integration with manufacturers, wholesale, shipping, etc.
* Compliance: Medical device manufacturers and pharmaceuticals face high reporting burdens to ensure patient safety, so aggregating supply chain data into one system helps streamline compliance – For example, [FarmaTrust’s](https://www.farmatrust.com/pharmaceutical-tracking-data) blockchain based system provides automated law enforcement notifications when they spot an issue
* Supply chain optimisation: Once all the data is in one place, companies apply AI to better predict demand and optimise supply accordingly

**Figure 1: FarmaTrust’s track and trace app for healthcare supply chains**



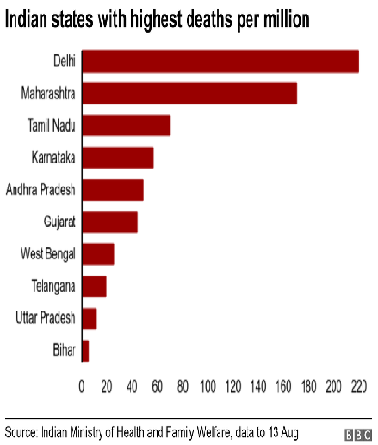
Source: FarmaTrust

Outside of financial markets, supply chain management and transparency is one of the most advanced use cases for blockchain, for example including the high profile partnership between [IBM and Walmart](https://www.forbes.com/sites/biserdimitrov/2019/12/05/how-walmart-and-others-are-riding-a-blockchain-wave-to-supply-chain-paradise/#398ecc597791) to ensure food safety in the supply chain. As the technology and ROI has already been proven, we expect this to be the most significant short-term impact of blockchain on the healthcare industry.

### 2. Patient-centric electronic health records

Healthcare systems[1] in every country and region are struggling with the problem of data siloes, meaning that patients and their healthcare providers have an incomplete view of medical histories. In 2016, Johns Hopkins University published research showing that [the third leading cause of death in the US was medical errors](https://www.hopkinsmedicine.org/news/media/releases/study_suggests_medical_errors_now_third_leading_cause_of_death_in_the_us) resulting from poorly coordinated care, such as planned actions not completed as intended or errors of omission in patient records.

**Figure 2:**



One potential solution to this problem is creating a blockchain-based system for medical records that can be linked into existing electronic medical record software and act as an overarching, single view of a patient’s record. It is crucial to emphasize that actual patient data does not go on the blockchain, but that each new record appended to the blockchain, whether a physician’s note, a prescription or a lab result, is translated into a unique hash function – a small string of letters and numbers. Every hash function is unique, and can only be decoded if the person who owns the data – in this case, the patient – gives their consent.

In this scenario, every time there is an amendment to a patient record, and every time the patient consents to share part of their medical record, it is logged on the blockchain as a transaction. [Medicalchain](https://medicalchain.com/en/) is a leading example of a company working with healthcare providers to implement blockchain enabled EMRs.

The key benefits of blockchain-enabled EMRs are:

A comprehensive single source of truth of a patient’s medical records, creating a better experience for patients and healthcare providers

They enable patients to see every time their medical records are updated and to give explicit consent every time they are shared with healthcare providers or others. Patients can also choose to share their medical records (or part of their medical records) with researchers and set time limits on how long any third party can have access to their medical information.

Medical insurers can receive immediate, validated confirmation of healthcare services directly from patients, without the time and cost of an intermediary

Beyond creating blockchain-based medical records, Medicalchain is also developing a platform upon which others can build digital health solutions, including a virtual consultation service and a medical data exchange, where patients can choose to sell their anonymised medical data, in exchange for Medtokens, to support digital health application development, e.g. population level analytics solutions.

The emergence of much more complete, digitised and shareable patient health records will have a profound impact on the healthcare market by fuelling more advanced analytics. For example, personalised medicine is a promising field, but its development is severely hindered by lack of enough high quality data. Access to more reliable and widespread population level data would enable much more powerful segmentation and analysis of targeted medicine outcomes.

Alongside its supply chain solution, FarmaTrust has developed a solution to support gene and cell therapy treatments, while many research programmes are also exploring how to combine AI and blockchain to drive forward personalised medicine (see here and here).

### 3. Smart contracts for insurance and supply chain settlements

### Blockchain-based[2] companies systems where various players in the healthcare sector, such as pharmaceutical companies, medical device OEMs, wholesalers, insurers and healthcare providers, can authenticate their identities as organisations, log contract details, and track transaction of goods and services, and payment settlement details for those goods and services. This type of environment goes a step beyond supply chain management to also enable trading partners and insurance providers in the healthcare sector to operate based on fully digital and in some cases automated contract terms.

By having shared digital contracts between manufacturers, distributers[8] and healthcare organisations logged on a blockchain ledger, rather than each player having their own version of contracts, they can significantly reduce disputes over payment chargeback claims for prescription medicines and other goods. According to Chronicled, because pricing structures often change, there are over one million chargeback claims made between these players every year, more than 5% of which are disputed, requiring lengthy manual resolution.

Similarly, shared smart contracts can be used to manage medical insurance contracts for patients, where Curisium states that 10% of claims are disputed. Like in other use cases, once this data is digitised and easily accessible, insurance providers can use more advanced analytics to optimise health outcomes and costs.

### 4. Medical staff credential verification

Similar to tracking the provenance of a medical good, blockchain technology can be used to track the experience of medical professionals, where trusted medical institutions and healthcare organisations can log the credentials of their staff, in turn helping to streamline the hiring process for healthcare organisations. US based [ProCredEx](https://procredex.com/how-it-works/) has developed such a medical credential verification system using the R3 Corda blockchain protocol.

The key benefits of the blockchain system are:

* Faster credentialing for healthcare organisations during the hiring process
* An opportunity for medical institutions, insurers, and healthcare providers to monetise their existing credentials data on past and existing staff
* Transparency and reassurance for partners, e.g. organisations sub-contracting locum tenens, or in emerging virtual health delivery models to inform patients on medical staff experience

### 5. IoT security for remote monitoring

One of the biggest trends[4][3] in digital health is the adoption of remote monitoring solutions, where all kinds of sensors measuring patients’ vital signs are being used to help give healthcare practitioners more visibility into patients’ health, enabling more proactive and preventative care. We’ve previously covered many promising remote monitoring use cases in our articles on [5G](https://stlpartners.com/digital-health-telecoms/10-5g-healthcare-use-cases/) and [edge computing](https://stlpartners.com/digital-health-telecoms/digital-health-at-the-edge/) in digital health.

However, security is a huge issue in health IoT,[10] both in terms of ensuring that patient data is private and secure and that it is not tampered with to create false information. In some cases, where a connected device may be depended on in emergency situations, e.g. alerting an elderly person’s carer that they have suffered a fall or a heart attack, it is also crucial that the supporting systems are very resilient to DDoS or other attacks disrupting service.

How blockchain systems could help secure remote monitoring IoT devices:

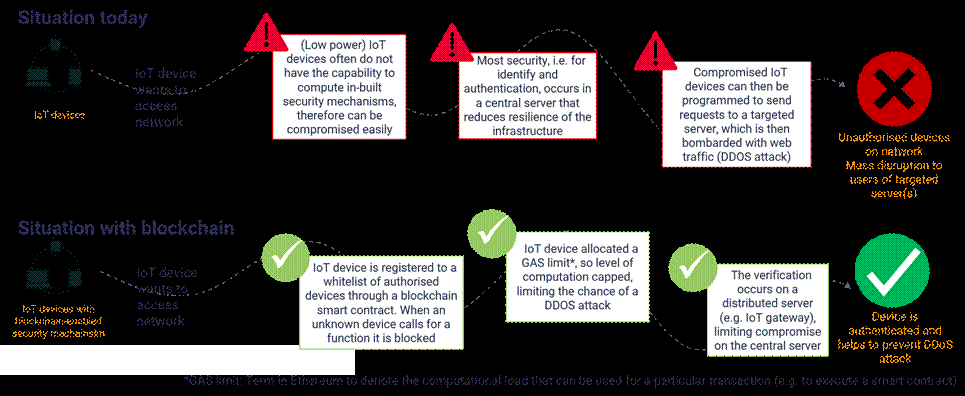
Blockchain cryptography ensures[7] that only permitted parties can gain access to personal data, which is stored on the blockchain as a unique hash function (any change in the source data will create a different hash function, and a user must have a specific set of cryptographic keys to decode the hash function into the source data)

Once patient data is recorded on the blockchain ledger (as a hash function) then it is nearly impossible to tamper with since it would require gaining access to all stored copies

The decentralised nature of blockchain means that IoT devices can interact directly with each other, without going through a centralised server (as most IoT connections do today), making it very difficult to launch DDoS and man in the middle attacks[10].

While blockchain could enhance IoT security in healthcare,[6][5] these use cases are still in the early stages of development and it is not yet clear whether blockchain will be the best tool to use. For digital health companies exploring how to ensure the security of remote monitoring devices, it is worth exploring blockchain, but only as part of a much more comprehensive end-to-end security strategy[9].

**Figure 3: How blockchain can improve IoT security**



## Referrence:

1. K. Nagarathna “Block chain based Malware Detection using Machine Learning Algorithms for IoT enabled E-Health Applications.” Vol.10 , Issue 11, Pages: 73-82, DOI: 10.48047/IJIEMR/V10/I11/12
2. MazinAlshamrani "IoT and artificial intelligence implementations for remote healthcaremonitoring systems: A survey", (https://doi.org/10.1016/j.jksuci.2021.06.005), 2021
3. SUDEEP TANWAR 1, QASIM BHATIA 1, PRUTHVI PATEL1, APARNA KUMARI1, PRADEEP KUMAR SINGH 2, AND WEI-CHIANG HONG 3" Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward"
4. Manoj M K , Thippa Reddy Gadekallu, Sivarama Krishnan S,NeerajKumar,SaqibHakak, Sweta Bhattacharya " Blockchain based Attack Detection on Machine Learning Algorithms for IoT based E- Health Applications",

(https://doi.org/10.1016/j.jksuci.2021.06.005), 2020

1. NasirEl Bassam, Distributed Renewable Energies for Off-Grid Communities (Second Edition) Empowering a Sustainable, Competitive, and Secure Twenty-First Century,(https://doi.org/10.1016/B978- 0-12-821605-7.00007-6) Chapter Twenty -

Blockchain 2021, Pages 447-450

1. D.Jeyabharathi, D.Kesavaraja, D.Sasireka, Handbook of Research on Blockchain Technology, Chapter 7 - Cloud-Based Blockchaining for Enhanced Security ([https://doi.org/10.1016/B978-0-](https://doi.org/10.1016/B978-0-12-819816-2.00007-1) [12-819816-2.00007-1](https://doi.org/10.1016/B978-0-12-819816-2.00007-1) ), 2020, Pages 171-181
2. Madhusudan Singh, ShihoKim, Advances in ComputersVolume 115, Chapter Four - Blockchain technology for decentralized autonomous organizations,([https://doi.org/10.1016/bs.adcom.2019](https://doi.org/10.1016/bs.adcom.2019.06.001)

[.06.001](https://doi.org/10.1016/bs.adcom.2019.06.001) ), 2019, Pages 115-140

1. A. Haleem, M. Javaid, Additive manufacturing applications in industry 4.0: a review, Journal of Industrial Integration and Management, 4 (4) (2019 Dec 4), Article 1930001
2. S. Perera, S. Nanayakkara, M.N.N. Rodrigo, S. Senaratne, R. Weinand, Blockchain technology: is it hype or real in the, construction industry?, Journal of Industrial Information Integration, 17 (2020), Article 100125
3. Jamil, F.; Hang, L.; Kim, K.; Kim, D. A novel medical blockchain model for drug supply chain integrity management in a smart hospital.Electronics 2019, 8, 505