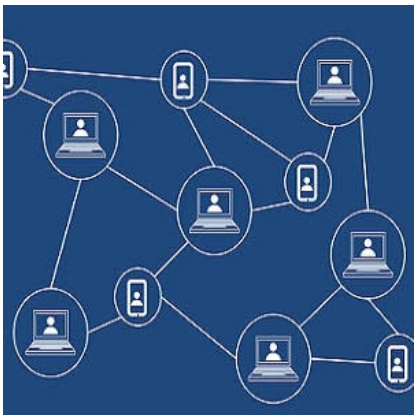
HealthManagement.org
Promoting Management and Leadership

Short read: smart contracts in healthcare



For researchers, funding plays an important role in accomplishing their work. In the healthcare industry, many relevant topics do not get sufficient funding because they are not profitable for pharmaceutical laboratories. Blockchain, which is based on distributed ledger technology, and "smart contracts" are seen as possible solutions to this funding problem.

"Blockchain will enable the crowdfunding of health-related research, thereby decoupling funding from business interest and linking it to social needs," says Simon Janin, software engineer and co-founder, chainSolutions GmbH, Zürich, Switzerland.

A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Funds that are raised for a research project, for example, can be held in a smart contract – which specifies the rules on how the money can be spent. The smart contract is self-enforcing and each party to this contract knows how the contract will behave, thus enabling higher trust levels, Janin explains.

Blockchain also offers a way of decentralising information without compromising integrity and security. A key aspect of decentralisation is the use of “reputation systems”, which can be implemented on blockchains in a transparent way.

Blockchain is a digital ledger in which transactions made in bitcoin or another cryptocurrency ("token") are recorded chronologically and publicly. "One can imagine a marketplace for medical research where researchers would be awarded reputation, in the form of a token, proportionally to the quality of their research," says Janin. "This can naturally be extended to reputation-based diagnostics; a patient answers targeted questions and provides his medical data, then a pool of trusted doctors provide independent diagnostics and collegially agree on a final diagnostic."

More generally, Janin explains, a healthcare prediction market could be established in which actors (i.e., doctors) that are correct more often are rewarded in a transparent way.

With the introduction of blockchain and smart contracts, the urgent need for privacy within peer-to-peer interactions has increased interest in the so-called "zero-knowledge proof" concept. Since most healthcare applications of blockchain also require privacy, zero-knowledge proofs are a force to be reckoned with, according to Janin.

A zero-knowledge proof can be viewed as a mathematical programme, or statement, that should convince anyone that a specific piece of data has some property, yet no information about that data should be leaked except for this property itself.

A direct use case for zero-knowledge proofs in the context of electronic health records (EHR) is the anonymous querying and aggregation of health data that preserves patients' anonymity entirely.

"We do not just render [the patients'] identity pseudonymous, which is known to leak personal information. Instead, we use a Zero-Knowledge protocol to entirely encipher patients' data," Janin points out. "We do this in such a way that, for example, aggregate data can be extracted out of the database, yet no actor can access all that data directly without the explicit consent of each single patient."

Giving patients control over their data will consist of blockchain technology and cryptographic techniques, says Janin, who adds that the data can also be watermarked so that data leaks can be traced back to the culpable source.

Source: HealthManagement.org
Image Credit: Pixabay

Published on : Wed, 22 Aug 2018