HealthManagement
Promoting Management and Leadership

Volume 18 - Issue 1, 2018 - Cover Story

Smart contracts in healthcare

Simon Janin
******@***chainsolutions.com

Software Engineer and co-founder,
chainSolutions GmbH, Switzerland

Looking at the future of Smart Contracts in healthcar e.

Could Smart Contract-enabled blockchains help protect patient data while also promoting watertight agreements in healthcare?

How Blockchain and Smart Contracts will impact the funding of research and innovation in healthcare

Definitions

- Blockchain: A digital ledger in which transactions made in bitcoin or another cryptocurrency are recorded chronologically and publicly
- Smart Contract: A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract
- Decenetralisation: Decentralisation is the process of distributing or dispersing function, powers, people or things away from a central location or authority

Across different industries, the funding process for research and development can be markedly disparate. In the healthcare industry, many relevant topics do not get sufficient funding because they are not profitable for pharmaceutical laboratories. Blockchain will enable the crowdfunding of health-related research, thereby decoupling funding from business interest and linking it to social needs.

Blockchains, especially Smart Contract-enabled blockchains like Ethereum, make it possible to create “tokens”. Tokens can be seen as new digital currencies whose rules can be chosen with great flexibility. Those tokens can be natively sold on the blockchain platform for other tokens - which creates a token economy. Initial Coin Offerings (ICOs) enable anyone to start an auction for tokens (or coins) they created - the process is virtually instantaneous and several millions can be raised within a few minutes. The funds are held in a Smart Contract; the rules according to which this money can be spent are specified and the smart contract is self-enforcing. Everyone knows how the contract will behave, thereby enabling higher trust levels.

Another key aspect of decentralisation is the use of “reputation systems”, which can be implemented on blockchains in a transparent way. 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. 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. This can further be enhanced with machine learning techniques, like DeepMind Health. More generally, a healthcare prediction market could be built in which actors that are correct more often are rewarded in a transparent way.

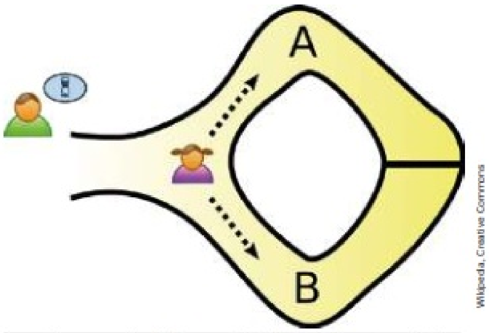
Zero-knowledge proofs (of knowledge)

Zero-knowledge proofs were initially an obscure field of research reserved to a few high-level computer scientists. Since the introduction of Smart Contracts and Blockchain, the urgent need for privacy within peer-to-peer interactions brought Zero-Knowledge proofs to the forefront.

Since most healthcare applications of blockchain also require privacy, zero-knowledge proofs are a force to be reckoned with.

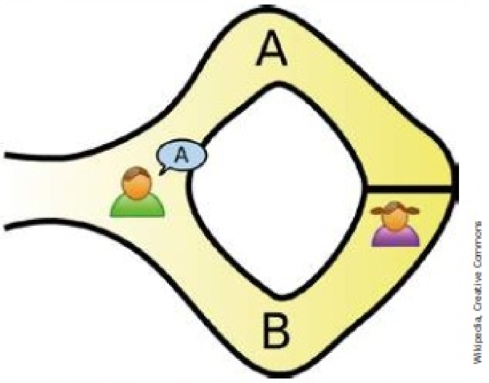
A zero-knowledge proof can be viewed as a mathematical programme, or statement, that should convince anyone that a specific piece of data has some property, yet no information about that data should be leaked except for this property itself. For example, a patient looking to buy insurance could give a proof that he has been diagnosed healthy by a certified doctor, without revealing who this doctor is. The patient would thereby lower his premium while the doctor’s identity remains protected. The applications of zero-knowledge proofs are extremely wide reaching. To give the reader an intuition about how they work, we illustrate them through the “Ali Baba’s cave” metaphor, initially presented by Jean-Jacques Quisquater in "How to Explain Zero-Knowledge Protocols to Your Children." To demonstrate, we will label the two parties in a zero-knowledge proof as Peggy (the prover of the statement) and Victor (the verifier of the statement).

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 their identity pseudonymous, which is known to leak personal information. Instead, we use a Zero-Knowledge protocol to entirely encipher patients’ data. 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.



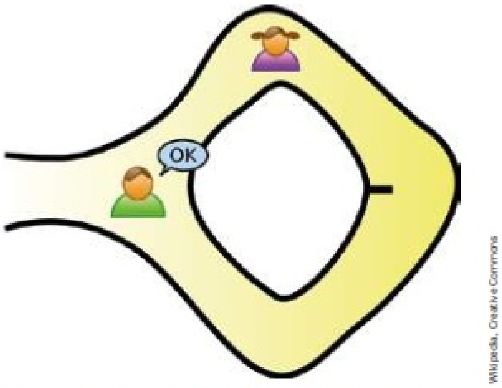
Wikipedia, Creative Commons

Peggy, the prover, randomly chooses path A or B. Victor does not see which one Peggy chooses.



Wikipedia, Creative Commons

Once Peggy is inside the cave, Victor (the verifier) chooses an exit at random and challenges Peggy to come out of it. Assuming Victor chooses exit A, Peggy can only come out if she has the key -- Note that the path from A to B is locked,. If Victor chooses B instead, Peggy can come out without knowing the key.
The key symbolises the secret that Peggy needs to know in order to be able to answer Victor’s challenge (i.e. unlock the door).



Wikipedia, Creative Commons

Peggy comes out of the exit that Victor chose. The likelihood of this happening even when Peggy does not have the key is 50 percent. We therefore run the protocol iteratively until that probability becomes small enough. This means that, in the next round, the probability of false positive is 25 percent, then 12.5 percent and so forth for each additional round. After 80 rounds, the probability of Peggy fooling Victor becomes less than 10^{-24} - so Peggy cannot cheat Victor.

Electronic Health Records: Giving patients more control over their data

The patients’ medical records are very valuable in two critical ways. Firstly, their structure and contents can make or break a diagnosis and they are critical for avoiding administering substances a patient is allergic to. Secondly, patient health data can be exploited for marketing purposes or even malicious purposes by external actors, which is why it is so critical to protect this data. Giving patients control over their data will consist of a mix of blockchain technology and recent cryptographic techniques.

To be clear, once data has been sent to an actor, there is no way to guarantee that this data is not copied or transmitted. Nonetheless, patients can require actors and institutions to sign a commitment that they will remove their data once the initial purpose for receiving them has been fulfilled. This is easy to do: the institution digitally signs a message containing the commitment and the patient keeps this commitment (some external server could store it as well). If the institution uses the data against the consent of the patient, the signature can serve as exhibit in court.

The data can be tainted in some identifiable way, also known as watermarking, so that leaking it can be traced back to the guilty party.

Drug provenance and integrity
According to Forbes, pharmaceutical companies incur an estimated annual loss of $200 billion due to counterfeit drugs globally (Forbes 2017). Using blockchain and Smart Contracts, it is possible to trace drugs over their whole life cycle. Each ingredient and substance is to be numbered and tracked, with geographic and other relevant information. The tracking data is then added to the blockchain (only the metadata is put in the blockchain for efficiency reasons).

The blockchain guarantees that this data cannot be compromised or removed; giving us the cryptographic property known as non-repudiability: once a drug has been tracked and registered, it is not possible for a malicious actor to make it disappear without getting caught.

Key Points

- A smart contract is a computer protocol intended to digitally implement a contract
- Decentralisation is the process of distributing functions and/or powers away from a central authority
- “Reputation Systems” support transparent implementation of decentralisation
- Giving patients control over their data will consist of blockchain technology and cryptographic techniques
- Data can be watermarked so that data leaks can be traced back to the culpable source
- Zero-Knowledge proofs and Blockchain combined offer trust and privacy
- Blockchain guarantees that data cannot be tampered with.

Published on : Thu, 25 Jan 2018