CIO

IDG CONTRIBUTOR NETWORK Want to Join?

THE NEXT GENERATION OF HEALTH IT

By Peter B. Nichol ★ Advisor

OPINION

Interactive and zero-knowledge proofs for better patient interactions with blockchain technology

Zero-knowledge proofs, when combined with blockchain technologies running on smart contracts, have the potential to prove patient health information without the verifier ever learning anything except that a statement is true.

CIO | Sep 1, 2016 6:00 AM PT

LIKE THIS ARTICLE? +2

Imagine for a minute all the healthcare situations where proof is required. Proof of a patient's healthcare coverage. Proof of a patient's name. Proof of a patient's medical history. Proof of a patient's prescription. Each question could be answered without the verifier (hospital receptionist, doctor or pharmacist) knowing anything except that the statement you told them was true. This is the power of zero-knowledge proofs.

Ideation of zero-knowledge proofs

In 1985, three researchers — Shafi (MIT), Micali (MIT) and Rackoff (University of Toronto) — drafted a paper titled "The Knowledge Complexity of Interactive Proof-Systems." Their research introduced first a theorem-proving procedure; a new efficient method of communicating a proof. The second part of the paper addressed the following question: *How much knowledge should be communicated for proving a theorem T?*

We are attempting to convince a verifier of the truth. The idea behind zero-knowledgeness is that the verifier does not learn anything except that a statement is true. What exactly does "does not learn anything" mean? Questions must be answered to formally define the zero-knowledgeness property. The specifics of zero-knowledgeness properties are explained in a good summary paper. Also, due to the math required to adequately explain the concepts of the zero-knowledgeness properties, I will not be covering the math here. We will focus on broader applications for healthcare. For now, you'll have to take my word for it: The math plays out.

Principles of zero-knowledge proofs

Zero-knowledge proofs have three important properties: completeness, soundness and zero-knowledge.

1. **Completeness:** The verifier always accepts the proof if the fact is true and both parties follow the protocol.
2. **Soundness:** The verifier always rejects the proof if the fact is false, as long as the verifier follows the protocol.
3. **ZeroKnowledge:** The verifier learns nothing else about the fact being proved from the prover that couldn't be learned without the prover, regardless of following the protocol. The verifier cannot even prove the fact to anyone later.

By leveraging blockchain technologies and smart contracts, we can ensure both parties follow the protocol.

Applying zero-knowledge proofs to healthcare

Let's apply this to healthcare. As you recall the initial question presented by Shafi, Micali and Rackoff (collectively referred to as SMR) was, "*How much knowledge should be communicated for proving a theorem T?"* We can restate this question to be patient-centric and healthcare-specific:

1. How much information does a hospital receptionist require on a patient to check the patient into the facility (hospital, provider or other)?
2. What are the minimum pieces of information required to share with a hospital receptionist to demonstrate a patient's proof of valid health insurance?
3. Is it possible to share no personal patient information (think the name, DOB, driver's license), and still have a pharmacist confirm you're able to pick up the prescription with the assurance you're the correct patient?

An interactive and zero-knowledge proof is a protocol between two parties in which one party, called the *prover*, tries to prove a particular fact to the other party, called the *verifier*. This concept is used for identification and authentication. Let's look at our three questions again, now considering the role of the verifier and prover.

1. How much information does a hospital (*verifier*) receptionist require on a patient (*prover*) to check the patient into the facility (hospital, provider, or other)?
2. What are the minimum pieces of information required to share with a hospital receptionist (*verifier*) to demonstrate a patient's (*prover*) proof of valid health insurance?
3. Is it possible to share no personal patient information (think the name, DOB, driver's license), and still have a pharmacist (*verifier*) confirm you're able to pick up the prescription with the assurance you're the correct patient (*prover*)?

Zero-knowledge proofs in practice

Most zero-knowledge proofs are based on a conversation between the prover and the verifier. This conversation occurs in a series of simulations or interactions, and they progress typically over iterations:

1. Commitment message from the prover.
2. Challenge from the verifier.
3. Response to the challenge from the prover.

Often this protocol repeats for several rounds. Then the verifier eventually decides whether to accept or reject the proof, based on the prover's responses in all the rounds.

The proof can also be performed efficiently by a simulator that has no idea of what the proof is.

The vision

A patient with an Android phone or an iPhone could use a decentralized application (dapp) to validate patient information during a healthcare event.

Dapps are the simplest form of a smart contract. This is an agreement involving digital assets between two parties that get automatically redistributed based on the contracted formula. In our case, this contract could release information to the verifier based on our zero-knowledge proof smart contract. At the end of the transaction, the verifier would agree that the statement was true — for example, the patient does have medical coverage required for the visit — but without conveying any information apart from the fact that the statement is indeed true.

Proving that one has a knowledge of certain information is trivial if one is allowed to directly reveal that information. Knowledge without knowledge — that's the next generation of patient interactions.

This article is published as part of the IDG Contributor Network. Want to Join?

Peter B. Nichol

★ **Advisor** | **IDG CONTRIBUTOR NETWORK**

Peter B. Nichol is a healthcare business and technology executive, who has been recognized for digital innovation by CIO.com, the MIT Sloan School of Management, Computerworld and the Project Management Institute.

Download the State of the CIO 2016 report

View Comments

How To Track Your Vehicle On The
Your News Online

6x Lotto Winner: Lottery Isn't
The Solutionaire

(1) Easy Trick "Removes" Your Eye Bags
Daily Tiply

"Shark Tank" Star Reveals Brilliant
OneSmartPenny

25 Unbelievable Facts About
POP Hitz

Anxiety? Cannabis Extract, Now
Healthy Report

Whaling emerges as major

Hybrid tablets will continue to grow in

New Rule In Austin, TX
Improve Insurance