Using Bitcoin to prevent identity theft

May 24 2017, by Larry Hardesty

"Our paper is about using Bitcoin to prevent online services from getting away with lying," says MIT graduate student Alin Tomescu. Credit: Christine Daniloff/MIT

A reaction to the 2008 financial crisis, Bitcoin is a digital-currency scheme designed to wrest control of the monetary system from central banks. With Bitcoin, anyone can mint money, provided he or she can

complete a complex computation quickly enough. Through a set of clever protocols, that computational hurdle prevents the system from being coopted by malicious hackers.

At the IEEE Symposium on Security and Privacy this week, researchers from MIT's Computer Science and Artificial Intelligence Laboratory are presenting a new system that uses Bitcoin's security machinery to defend against online identity theft.

"Our paper is about using Bitcoin to prevent online services from getting away with lying," says Alin Tomescu, a graduate student in electrical engineering and computer science and first author on the paper. "When you build systems that are distributed and send each other digital signatures, for instance, those systems can be compromised, and they can lie. They can say one thing to one person and one thing to another. And we want to prevent that."

An attacker who hacked a public-key encryption system, for instance, might "certify"—or cryptographically assert the validity of—a false encryption key, to trick users into revealing secret information. But it couldn't also decertify the true key without setting off alarms, so there would be two keys in circulation bearing certification from the same authority. The new system, which Tomescu developed together with his thesis advisor, Srini Devadas, the Edwin Sibley Webster Professor of Electrical Engineering and Computer Science at MIT, defends against such "equivocation."

Because Bitcoin is completely decentralized, the only thing ensuring its reliability is a massive public log—referred to as the blockchain—of every Bitcoin transaction conducted since the system was first introduced in 2009. Earlier systems have used the Bitcoin machinery to guard against equivocation, but for verification, they required the download of the entire blockchain, which is 110 gigabytes and growing

hourly. Tomescu and Devadas' system, by contrast, requires the download of only about 40 megabytes of data, so it could run on a smartphone.

Striking paydirt

Extending the blockchain is integral to the process of minting—or in Bitcoin terminology, "mining"—new bitcoins. The mining process is built around a mathematical function, called a one-way hash function, that takes three inputs: the last log entry in the blockchain; a new blockchain entry, in which the miner awards him- or herself a fixed number of new bitcoins (currently 12.5); and an integer. The output of the function is a string of 1s and 0s.

Mining consists of trying to find a value for the input integer that results in an output string with a prescribed number of leading 0s—currently about 72. There's no way to do this except to try out lots of options, and even with a huge bank of servers churning away in the cloud the process typically takes about 10 minutes. And it's a race: Adding a new entry—or "block"—to the blockchain invalidates the most recent work of all other miners, who now have to start over using the newly added block as an input.

In addition to assigning the winning miner the latest quota of bitcoins, a new block in the blockchain also records recent transactions by Bitcoin users. Roughly 100,000 commercial vendors in the real world now accept payment in bitcoins. To verify a payment, the payer and vendor simply broadcast a record of their transaction to the Bitcoin network. Miners add the transaction to the blocks they're working on, and when the transaction shows up in the blockchain, it's a matter of public record.

The transaction record also has room for an 80-character text annotation. Eighty characters isn't enough to record, say, all the public keys certified

by a public-key cryptography system. But it is enough to record a cryptographic signature verifying that a certification elsewhere on the Internet is legitimate.

Previous schemes for preventing equivocation simply stored such signatures in the annotations of transaction records. Bitcoin's existing security structure prevents tampering with the signatures.

But verifying that a Web service using those schemes wasn't equivocating required examining every transaction in every block of the blockchain—or at least, every block added since the service first used the scheme to certify a public assertion. It's that verification process that Tomescu and Devadas have refined.

Efficient audits

"Our idea is so simple—it's embarrassingly simple," Tomescu says. The central requirement of Bitcoin is that no one can spend the same bitcoin in more than one place, and the system has cryptographic protocols in place to prevent that from happening.

So Tomescu and Devadas's system—called Catena—simply adds the requirement that every Bitcoin transaction that logs a public assertion must involve an actual bitcoin transfer. Users may simply transfer the bitcoin to themselves, but that precludes the possibility of transferring the bitcoin to anyone else in the same block of the blockchain. Consequently, it also precludes equivocation within the block.

To prevent equivocation between blocks, it's still necessary to confirm that the bitcoin that the Catena user spends in one block is the same one that it spent the last time it made a public assertion. But again, because the ability to verify a bitcoin's chain of custody is so central to the success of the whole Bitcoin system, this is relatively easy to do. People

who want to use Catena to audit all the public assertions of a given Web service still need to download information from every block of the blockchain. But they need to download only a small cryptographic proof—about 600 bytes—for each block, rather than the block's full megabyte of data.

"The abstraction that the paper lays out is a really good idea—the idea of making it possible to create, you might say, smaller blockchains or linked lists within a blockchain specific to a particular account or a particular object," says Bryan Ford, an associate professor of computer science at the Swiss Federal Institute of Technology in Lausanne. "It's very cool, nice, clean, useful primitive, clearly explained. It's very synergistic with an idea we've been working on, which creates an efficiently traversable timeline, which we call a skip chain, meaning a timeline you can skip around on arbitrarily forward and back, where from any point you can verify any other point in the timeline very efficiently."

"If you can eliminate the possibility of equivocation, it becomes easier to secure many algorithms," he adds. "It's a generally important problem."

More information: Catena: Efficient Non-equivocation via Bitcoin: people.csail.mit.edu/alinush/p … rs/catena-sp2017.pdf

Provided by Massachusetts Institute of Technology