Towards sustainable blockchains

May 4 2018

Award ceremony at Eurocrypt 2018: Krzysztof Pietrzak (left) und Bram Cohen (second from left) receive the Best Paper Award from Eurocrypt-chair Jesper Buus Nielsen (right). Credit: IST Austria

As blockchains become ever more popular and widespread, a growing concern is their sustainability. Current designs, most notably the blockchain underlying the Bitcoin cryptocurrency, are secured using so-

called "proofs of work," which requires huge amounts of computational power. This is an ecological problem challenging the long-term viability of cryptocurrencies. In an ongoing collaboration, Institute of Science and Technology Austria (IST Austria) Professor Krzysztof Pietrzak and BitTorrent inventor/Chia Network CEO Bram Cohen seek to address this problem by making use of disk space rather than computational work. Research into one of the two key components of this approach—"proofs of sequential work," also known as "verifiable delay algorithms," received this year's Best Paper Award at EUROCRYPT, one of the world's top two cryptography conferences.

Bitcoin is by far the most successful digital currency. Its decentralized nature distinguishes it from all previously proposed digital currencies. Instead of having a central entity, all Bitcoin transactions are recorded in a public sequence of blocks known as a blockchain. To add a block to the blockchain, a user (or "miner") needs to provide a "proof of work," that is, they must solve a kind of cryptographic puzzle or challenge. As long as more than half of the computational power dedicated toward solving these puzzles is contributed by honest parties, the blockchain acts as robust, non-tamperable ledger that keeps track of all the Bitcoin transactions. Miners are incentivized by the promise of receiving Bitcoins as a reward for adding blocks, currently worth about U.S. $100,000 (about EUR 80,000) for every block found. This leads to massive energy use—by some estimates, the equivalent consumption of Denmark. But the problem is not only ecological, it is also economical. The high rewards required to incentivize miners will, in the long run, lead either to inflation or high transaction costs.

,

Researchers have been looking into alternatives to proofs of work for securing blockchains. "We believe the most promising approach is to use disk space," says Krzysztof Pietrzak. "There exist massive amounts of unused disk space—in data centers, but also personal laptops and the like—which could be used for mining at almost no marginal cost."

Designing blockchains that use disk space instead of proofs of work is a challenging problem. A recent proposal, the Chia network (chia.net), will replace proofs of work with two key components.

The first of these is "proofs of space," which are used by miners to prove they dedicate disk space. As those proofs are extremely cheap to generate once the dedicated space has been initialized, another component is required to enforce a dynamic in which new blocks only appear every few minutes, similar to what occurs in Bitcoin. This second component uses what is called a "proof of sequential work" or "verifiable delay algorithm." Essentially, this is a protocol where the user can show that they have done a long sequential computation upon receiving some sort of challenge. Being sequential means that—unlike "normal" proofs of work—having enormous amounts of computational power available does not make the computation any faster. Therefore, it serves as proof that a given amount of time has elapsed since the challenge has been received.

In their award-winning paper, Cohen and Pietrzak construct the first practical and publicly verifiable proof of sequential work. Previous constructions either require the verifier to hold a secret trapdoor to verify a proof, or the prover to dedicate a massive amount of disk space to generate a proof.

Existing algorithms were extremely complicated, or the proofs could only be verified by a party that had some kind of secret trapdoor, or the prover required a massive amount of disk space to generate a proof. Unfortunately, the new construction cannot be readily used for the main application the authors were interested in—blockchain designs—as it lacks one crucial property: uniqueness. In particular, a valid proof can be adapted into a different valid proof without having to repeat the sequential computation. This is a problem since the process to add a new block is like a lottery, and without the uniqueness property, an adversary

could generate many different proofs of sequential work, and only announce the one that gives him the best chance of also winning this lottery in the next round. "Coming up with a design where proofs have a canonical representation without using heavy cryptographic machinery is an exciting open question," says Pietrzak.

Provided by Institute of Science and Technology Austria