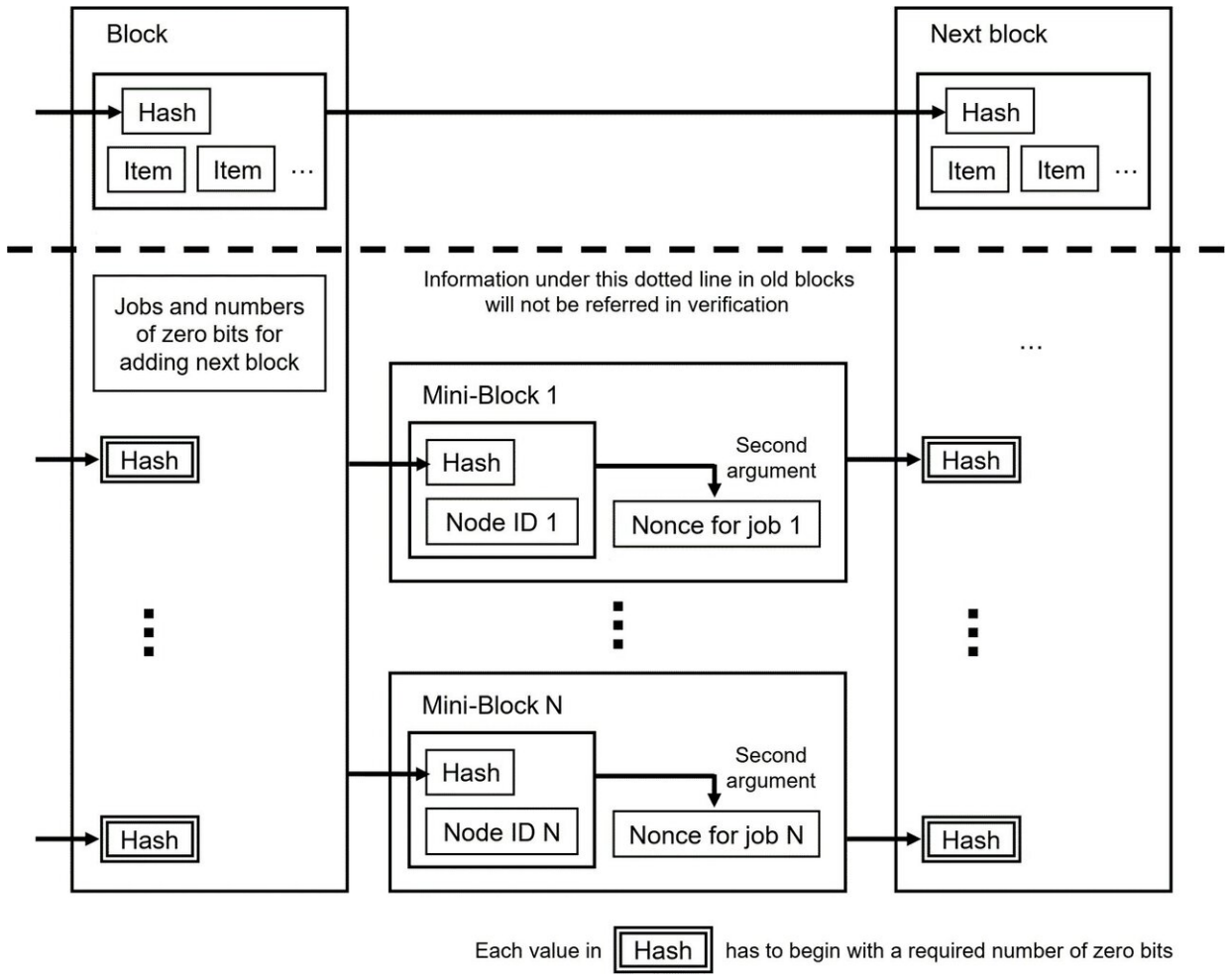
All Bitcoin mining should be environmentally friendly

December 10 2019



The data structure of a block in a blockchain with the proposed protocol. Credit: Naoki Shibata

The rise in popularity of cryptocurrencies such as Bitcoin has the potential to change how we view money. At the same time, governments and societies are worried that the anonymity of these cashless transactions could allow criminal activities to flourish. Another less remarked upon issue is the energy demands needed to mint new coins for these cryptocurrencies. A new report by Associate Professor Naoki Shibata of Nara Institute of Science and Technology presents a blockchain algorithm, which he calls "proof-of-search" (PoS), that retains the attractive features of most cryptocurrencies at a lower cost to the environment.

While the economics of cryptocurrencies gets most of the attention, it is becoming readily apparent that cryptocurrencies have a massive environmental cost. The energy used in the world to mine Bitcoins alone equals almost that of the energy consumption of all of Ireland, while in Iceland, Bitcoin mining consumes more energy than households. In the end, it could be environmental implications, not economic ones, that halt the mainstream adoption of cryptocurrencies.

The basis of all major cryptocurrencies is the blockchain. Ironically, while the blockchain provides pure anonymity to the human user, it is remarkably transparent in all its transactions, meaning the digital owner of the digital coins is clear, even if the actual person represented by the digital owner is not.

"Bitcoin uses a proof-of-work [PoW] system to decide the chronological order of transactions. PoW works anonymously because the order is identified by IP addresses," explains Shibata.

When a transaction in the Bitcoin blockchain is made, a user makes a request. PoW makes a series of calculations to confirm the validity of the transaction, calculations that consume energy. In PoS, users in the blockchain are invited to use this energy to request a job for finding a

solution to an optimization problem.

"There are three kinds of users in the PoS blockchain. The first two are those who want to use the blockchain as a payment system or mine for e-coins, which is the same as PoW. The third group wants to use the PoS blockchain as grid computing infrastructure," says Shibata.

The energy lost in the PoW is redirected to finding an approximate solution to the submitted problem. Thus, energy can be devoted to adding new blocks to the blockchain or to another problem, namely, the optimization proposed by a user, so that the amount of energy used is not reduced, but neither is it wasted.

PoS is the newest of more than a dozen alternative algorithms to PoW that all aim to reduce energy cost. PoW has remained the standard algorithm through which cryptocurrencies operate, because it is extremely decentralized and democratic, which prevents any one user from having an outstanding influence on the currency value.

"The problem with the alternatives is that they lose their democracy or are more vulnerable to outside attacks," notes Shibata.

By adding the feature of an approximate solution, PoS also invites possible corruption to which PoW is immune. Therefore, as a deterrent, PoS demands that the user who submits the problem be the one who pays the user who proposes the solution. This prevents users from colluding together to submit problems for which they already know the solution.

Another appeal of PoW is its robustness. PoS preserves this robustness by introducing miniblocks each time an optimization problem is submitted.

Shibata envisions the optimization problems that can be solved by redirecting the wasted energy with PoS will include diverse problems from medicine to the beginnings of the universe.

"PoS could help solve problems in protein folding, the dynamics of interstellar formations and finance," he says.

More information: Naoki Shibata, Proof-of-Search: Combining Blockchain Consensus Formation with Solving Optimization Problems, *IEEE Access* (2019). DOI: 10.1109/ACCESS.2019.2956698

Provided by Nara Institute of Science and Technology