Cryptography in the blockchain era

May 18 2022, by Stephanie Jones

Credit: CC0 Public Domain

The advent of blockchains has ignited much excitement, not only for their realization of novel financial instruments, but also for offering alternative solutions to classical problems in fault-tolerant distributed computing and cryptographic protocols. Blockchains are managed and built by miners and are used in various settings, the best known being a

distributed ledger that keeps a record of all transactions between users in cryptocurrency systems such as Bitcoin.

Underlying many such protocols is a primitive known as a "proof of work" (PoW), which for over 20 years has been liberally applied in cryptography and security literature to a variety of settings, including spam mitigation, sybil attacks and denial-of-service protection. Its role in the design of blockchain protocols, however, is arguably its most impactful application.

As miners receive new transactions, the data are entered into a new block, but a PoW must be solved to add new blocks to the chain. PoW is an algorithm used to validate Bitcoin transactions. It is generated by Bitcoin miners competing to create new Bitcoin by being the first to solve a complex mathematical puzzle, which requires very expensive computers and a lot of electricity. Once a miner finds a solution to a puzzle, they broadcast the block to the network so that other miners can verify that it's correct. Miners who succeed are then given a fixed amount of Bitcoin as a reward.

However, despite the evolution of our understanding of the PoW primitive, pinning down the exact properties sufficient to prove the security of Bitcoin and related protocols has been elusive. In fact, all existing instances of the primitive have relied on idealized assumptions.

A team led by Dr. Juan Garay has identified and proven the concrete properties—either number-theoretic or pertaining to hash functions. They were then used to construct blockchain protocols that are secure and safe to use. With their new algorithms, the researchers demonstrated that such PoWs can thwart adversaries and environments, collectively owning less than half of the computational power in the network.

Garay's early work on cryptography in blockchain was first published in

the Proceedings of Eurocrypt 2015, a top venue for the dissemination of cryptography research.

The techniques underlying PoWs transcend the blockchain context. They can, in fact, be applied to other important problems in the area of cryptographic protocols, thus circumventing well-known impossibility results, a new paradigm that Garay calls "Resource-Restricted Cryptography."

"It's a new way of thinking about cryptography in the sense that things do not have to be extremely difficult, only moderately difficult," said Garay. "And then you can still do meaningful things like blockchains. Cryptocurrencies are just one example. My work, in general, is understanding this landscape and coming up with the mathematics that explain it and make it work."

More information: Juan Garay et al, Blockchains from Non-Idealized Hash Functions, Proceedings of Eurocypt 2015, eprint.iacr.org/2014/765.pdf

Provided by Texas A&M University College of Engineering

Citation: Cryptography in the blockchain era (2022, May 18) retrieved 5 May 2024 from https://techxplore.com/news/2022-05-cryptography-blockchain-era.html