More efficient cryptocurrency reduces data needed to join the network and verify transactions by 99 percent

January 24 2019, by Rob Matheson

MIT researchers have developed a new secure cryptocurrency that reduces data users need to join the network and verify transactions by up to 99 percent, compared to today's popular cryptocurrencies, which could mean a more scalable network. Credit: Christine Daniloff

MIT researchers have developed a new cryptocurrency that drastically reduces the data users need to join the network and verify transactions—by up to 99 percent compared to today's popular cryptocurrencies. This means a much more scalable network.

Cryptocurrencies, such as the popular Bitcoin, are networks built on the blockchain, a financial ledger formatted in a sequence of individual blocks, each containing transaction data. These networks are decentralized, meaning there are no banks or organizations to manage funds and balances, so users join forces to store and verify the transactions.

But decentralization leads to a scalability problem. To join a cryptocurrency, new users must download and store all transaction data from hundreds of thousands of individual blocks. They must also store these data to use the service and help verify transactions. This makes the process slow or computationally impractical for some.

In a paper being presented at the Network and Distributed System Security Symposium next month, the MIT researchers introduce Vault, a cryptocurrency that lets users join the network by downloading only a fraction of the total transaction data. It also incorporates techniques that delete empty accounts that take up space, and enables verifications using only the most recent transaction data that are divided and shared across the network, minimizing an individual user's data storage and processing requirements.

In experiments, Vault reduced the bandwidth for joining its network by 99 percent compared to Bitcoin and 90 percent compared to Ethereum, which is considered one of today's most efficient cryptocurrencies. Importantly, Vault still ensures that all nodes validate all transactions, providing tight security equal to its existing counterparts.

"Currently there are a lot of cryptocurrencies, but they're hitting bottlenecks related to joining the system as a new user and to storage. The broad goal here is to enable cryptocurrencies to scale well for more and more users," says co-author Derek Leung, a graduate student in the Computer Science and Artificial Intelligence Laboratory (CSAIL).

Joining Leung on the paper are CSAIL researchers Yossi Gilad and Nickolai Zeldovich, who is also a professor in the Department of Electrical Engineering and Computer Science (EECS); and recent alumnus Adam Suhl '18.

Vaulting over blocks

Each block in a cryptocurrency network contains a timestamp, its location in the blockchain, and fixed-length string of numbers and letters, called a "hash," that's basically the block's identification. Each new block contains the hash of the previous block in the blockchain. Blocks in Vault also contain up to 10,000 transactions—or 10 megabytes of data—that must all be verified by users. The structure of the blockchain and, in particular, the chain of hashes, ensures that an adversary cannot hack the blocks without detection.

New users join cryptocurrency networks, or "bootstrap," by downloading all past transaction data to ensure they're secure and up to date. To join Bitcoin last year, for instance, a user would download 500,000 blocks totaling about 150 gigabytes. Users must also store all account balances to help verify new users and ensure users have enough funds to complete transactions. Storage requirements are becoming substantial, as Bitcoin expands beyond 22 million accounts.

The researchers built their system on top of a new cryptocurrency network called Algorand—invented by Silvio Micali, the Ford Professor of Engineering at MIT—that's secure, decentralized, and more scalable

than other cryptocurrencies.

With traditional cryptocurrencies, users compete to solve equations that validate blocks, with the first to solve the equations receiving funds. As the network scales, this slows down transaction processing times. Algorand uses a "proof-of-stake" concept to more efficiently verify blocks and better enable new users join. For every block, a representative verification "committee" is selected. Users with more money—or stake—in the network have higher probability of being selected. To join the network, users verify each certificate, not every transaction.

But each block holds some key information to validate the certificate immediately ahead of it, meaning new users must start with the first block in the chain, along with its certificate, and sequentially validate each one in order, which can be time-consuming. To speed things up, the researchers give each new certificate verification information based on a block a few hundred or 1,000 blocks behind it—called a "breadcrumb." When a new user joins, they match the breadcrumb of an early block to a breadcrumb 1,000 blocks ahead. That breadcrumb can be matched to another breadcrumb 1,000 blocks ahead, and so on.

"The paper title is a pun," Leung says. "A vault is a place where you can store money, but the blockchain also lets you 'vault' over blocks when joining a network. When I'm bootstrapping, I only need a block from way in the past to verify a block way in the future. I can skip over all blocks in between, which saves us a lot of bandwidth."

Divide and discard

To reduce data storage requirements, the researchers designed Vault with a novel "sharding" scheme. The technique divides transaction data into smaller portions—or shards—that it shares across the network, so

individual users only have to process small amounts of data to verify transactions.

To implement sharing in a secure way, Vault uses a well-known data structure called a binary Merkle tree. In binary trees, a single top node branches off into two "children" nodes, and those two nodes each break into two children nodes, and so on.

In Merkle trees, the top node contains a single hash, called a root hash. But the tree is constructed from the bottom, up. The tree combines each pair of children hashes along the bottom to form their parent hash. It repeats that process up the tree, assigning a parent node from each pair of children nodes, until it combines everything into the root hash. In cryptocurrencies, the top node contains a hash of a single block. Each bottom node contains a hash that signifies the balance information about one account involved in one transaction in the block. The balance hash and block hash are tied together.

To verify any one transaction, the network combines the two children nodes to get the parent node hash. It repeats that process working up the tree. If the final combined hash matches the root hash of the block, the transaction can be verified. But with traditional cryptocurrencies, users must store the entire tree structure.

With Vault, the researchers divide the Merkle tree into separate shards assigned to separate groups of users. Each user account only ever stores the balances of the accounts in its assigned shard, as well as root hashes. The trick is having all users store one layer of nodes that cuts across the entire Merkle tree. When a user needs to verify a transaction from outside of their shard, they trace a path to that common layer. From that common layer, they can determine the balance of the account outside their shard, and continue validation normally.

"Each shard of the network is responsible for storing a smaller slice of a big data structure, but this small slice allows users to verify transactions from all other parts of network," Leung says.

More information: Vault: Fast Bootstrapping for Cryptocurrencies. people.csail.mit.edu/nickolai/ … ung-vault-eprint.pdf

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology

Citation: More efficient cryptocurrency reduces data needed to join the network and verify transactions by 99 percent (2019, January 24) retrieved 1 May 2024 from https://techxplore.com/news/2019-01-efficient-cryptocurrency-network-transactions-percent.html