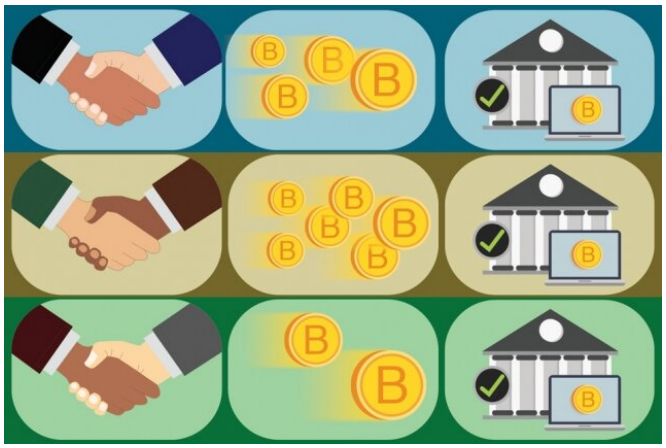
Giving cryptocurrency users more bang for their buck

30 January 2020, by Rob Matheson



Spider, a new cryptocurrency-routing scheme, splits each full transaction into smaller “packets” that are sent across different channels at different rates. Credit: Chelsea Turner, MIT

A new cryptocurrency-routing scheme co-invented by MIT researchers can boost the efficiency—and, ultimately, profits—of certain networks designed to speed up notoriously slow blockchain transactions.

Cryptocurrencies hold promise for peer-to-peer financial transactions, potentially making banks and credit cards obsolete. But there's a scalability issue: Bitcoin, for instance, processes only a handful of transactions per second, while major credit cards process hundreds or thousands. That's because the blockchain—the digital ledger cryptocurrencies are built on—takes a really long time to process transactions.

A new solution is "payment channel networks" (PCNs), where transactions are completed with minimal involvement from the blockchain. Pairs of PCN users form off-blockchain escrow accounts with a dedicated amount of money, forming a large, interconnected network of joint accounts. Users route payments through these accounts, only pinging the blockchain to establish and close the accounts, which speeds things up dramatically. Accounts can also collect a tiny fee when transactions get routed through them.

Inefficient routing schemes, however, slow down even these fast solutions. They deplete users' balances in these accounts frequently, forcing them to invest a lot of money in each account or frequently rebalance their accounts on the blockchain. In a paper being presented next month at the USENIX Symposium on Networked Systems Design and Implementation, the researchers introduce "Spider," a more efficient routing scheme that lets users invest only a fraction of funds in each account and process roughly four times more transactions before rebalancing on the blockchain.

"It's important to have balanced, high-throughput routing in PCNs to ensure the money that users put into joint accounts is used efficiently," says first author Vibhaalakshmi Sivaraman, a graduate student in the Computer Science and Artificial Intelligence Laboratory (CSAIL). "This should be efficient and a lucrative business. That means routing as many transactions as possible, with as little funds as possible, to give PCNs the best bang for their buck."

Joining Sivaraman on the paper are former postdoc Shaileshh Bojja Venkatakrishnan, CSAIL graduate students Parimarjan Negi and Lei Yang, and Mohammad Alizadeh, an associate professor of electrical engineering and computer science and a CSAIL researcher; Radhika Mittal of the University of Illinois at Urbana-Champaign; and Kathleen Ruan and Giulia Fanti of Carnegie Mellon University.

Packet payments

PCNs rely heavily on bidirectional joint accounts—where both parties can receive and send

money—so money can be routed between any users. User B can have a joint account with user A, while also linking separately to user C. Users A and C are not directly connected, but user A can send money to user C via the A-B and B-C joint accounts.

To exchange funds, each party must approve and update the balances in their joint accounts. Payments can only be routed on channels with sufficient funds to handle the transactions, causing major issues.

Traditional schemes send transactions along the shortest path possible, without being aware of any given user's balance or the rate of sending on that account. This can cause one of the users in the joint account to handle too many transactions and drop to a zero balance, making it unable to route further transactions. What's more, users can only send a payment in full. If a user wants to send, say, 10 bitcoins, current schemes try to push the full amount on the shortest path possible. If that path can't support all 10 bitcoins at once, they'll search for the next shortest path, and so on—which can slow down or completely fail the transaction.

Inspired by a technique for internet communications called packet switching, Spider splits each full transaction into smaller "packets" that are sent across different channels at different rates. This lets the scheme route chunks of these large payments through potentially low-funded accounts. Each packet is then far more likely to reach its destination without slowing down the network or being rejected in any given account for its size.

"Shortest-path routing can cause imbalances between accounts that deplete key payment channels and paralyze the system," Sivaraman says. "Routing money in a way that the funds of both users in each joint account are balanced allows us to reuse the same initial funds to support as many transactions as possible."

All queued up

Another innovation was creating queues at congested accounts. If an account can't handle incoming transactions that require it to send money, instead of rejecting them, it queues them up. Then, it waits for any transactions that will replenish its funds—within a reasonable time frame—to be able to process those transactions.

"If you're waiting on a queue, but I send you funds within the next second, you can then use any of those funds to send your waiting transactions," Sivaraman says.

The researchers also adopted an algorithm—built by Alizadeh and other researchers—that monitors data center congestion to identify queueing delays at congested accounts. This helps control the rate of transactions. Say user A sends funds to user C through user B, which has a long queue. The receiver C sends the sender A, along with the payment confirmation, one bit of information representing the transaction's wait time at user B. If it's too long, user A routes fewer transactions through user B. As the queueing time decreases, account A routes more transactions through B. In this manner, by monitoring the queues alone, Spider is able to ensure that the rate of transactions is both balanced and as high as possible.

Ultimately, the more balanced the routing of PCNs, the smaller the capacity required—meaning, overall funds across all joint accounts—for high transaction throughput. In PCN simulations, Spider processed 95 percent of all transactions using only 25 percent of the capacity needed in traditional schemes.

The researchers also ran tests on tricky transactions called "DAGs," which are one-directional payments where one user inevitably runs out of funds and needs to rebalance on the blockchain. A key metric for the performance of PCNs on DAG transactions is the number of off-chain transactions enabled for each transaction on the blockchain. In this regard, Spider is able to process eight times as many off-chain transactions for each transaction on-chain. In contrast, traditional schemes only support twice as many off-chain transactions.

"Even with extremely frequent rebalancing, traditional schemes can't process all DAG transactions. But with very low-frequency rebalancing, Spider can complete them all,"

Sivaraman says.

Next, the researchers are making Spider more robust to DAG transactions, which can cause bottlenecks. They're also exploring data privacy issues and ways to incentivize users to use Spider.

More information: High Throughput Cryptocurrency Routing in Payment Channel Networks, arXiv:1809.05088 [cs.NI]
arxiv.org/abs/1809.05088

Provided by Massachusetts Institute of Technology