GBBC Global Blockchain Business Council

Open Learning Forum

FlyClient: Super-Light Clients for Cryptocurrencies

Beneditk Bünz; Lucianna Kiffer; Loi Luu; and Mahdi Zamani
Stanford University; Northeastern University; Kyber Network; Visa Research
Date Published: 2/28/2019

Executive Summary written by GBBC

Problem

Traditional financial service providers currently have a distinct advantage over blockchain services: they can offer digital payment services on mobile phones and Internet of Things (IoT) devices. This is not possible with decentralized cryptocurrency networks like Bitcoin and Ethereum, which need nodes to confirm new blocks on their blockchains; the blockchain verification process requires a large amount of bandwidth and storage and is not practical on a mobile device.

While there are existing light clients, they are not sufficiently scalable to be feasible for mobile devices. For example, simplified payment verification (SPV) only downloads the headers of each block (for Bitcoin this is 80 bytes per block instead of the usual 1MB). However, the bandwidth and storage overhead increase linearly as the number of blocks increases. It is also necessary to redownload the data each time one wishes to process a transaction.

FlyClient

FlyClient enables individuals to verify a chain by sampling a logarithmic number of block headers, meaning the sample does not increase linearly but rather much more slowly. The individual would then only need to keep a single block to verify transactions, significantly reducing the necessary bandwidth and storage. In the experiment, researchers found that FlyClient can verify and create proofs in less than a second with limited bandwidth and storage. Unlike other advanced light clients, it is also able to handle the fluctuating difficulty of the Ethereum blockchain.

FlyClient can be used on proof-of-work blockchains like Bitcoin and Ethereum. It can also be used on proof-of-stake, proof-of-space, and proof-of-elapsed-time blockchains.

Requirements

Unfortunately, FlyClient cannot be deployed on Bitcoin and Ethereum as they are currently operating; it is necessary that nodes maintain a Merkle mountain range (MMR) over all blocks for sampling purposes. To achieve this on existing blockchains without MMRs, a soft or hard fork would be necessary.

Conclusion

FlyClient proves that it is possible to make seemingly bulky and slow blockchains agile and mobile. While FlyClient is not yet usable on Bitcoin or Ethereum, it and other advanced light clients are helping to chip away at traditional financial institutions' advantage in the digital payment space. With new blockchains being developed with light clients in mind, it will not be long before fast digital payment services on the blockchain are a reality.