GBBC Global Blockchain Business Council

# Open Learning Forum

## Scaling Nakamoto Consensus to Thousands of Transactions per Second

Chenxing Li; Peilun Li; Dong Zhou; Wei Xu; Fan Long; and Andrew Chi-Chih Yao
*Institute for Interdisciplinary Information Sciences, Tsinghua University*
Date Published: 8/31/2018

Executive Summary written by GBBC

### Introduction

Many blockchain platforms, including Bitcoin, use what is known as a *Nakamoto consensus*, which links transactions to previous transactions. To prevent alterations of previous transactions, nodes use the longest chain of blocks as the basis for future blocks. While this ensures a secure ledger of transactions, it also creates a bottleneck in which forks (concurrent blocks) are discarded; this slowness is vital to security. The bottleneck is most evident when users face long transaction confirmation delays and high transaction fees.

### Conflux

Conflux is a blockchain system that can confirm transactions in minutes using a protocol that allows faster block generation. This protocol is different in that it “defer[s] the transaction total ordering and optimistically process[es] concurrent transactions and blocks.” Essentially, Conflux uses the assumption that transactions will rarely conflict with one another across concurrent blocks. This means that instead of forming a chain with forks (which wastes time, energy, bandwidth, etc.), blocks are joined together into a direct acyclic graph (DAG). DAGs are a different form of distributed ledger technology, in which concurrent blocks are allowed to exist with one another, enabling the ledger to branch out like a tree rather than a linear chain. Conflux then orders concurrent blocks using a “pivot chain,” which sorts blocks into “epochs” with a novel ordering algorithm. This means Conflux can confirm blocks on the pivot chain using an altered Nakamoto consensus, eliminating the issues associated with DAG consensus.

### Results

Using full nodes with a bandwidth limit of 20Mbps, Conflux is able to process one 4MB block in 5 seconds; its 2.88GB/hour throughput is 11.62x that of Bitcoin. With a bandwidth limit of 40Mbps, Conflux can process one 4MB block in 2.5 seconds for a throughput of 5.76GB/hour. Experimental results showed that Conflux shifted the bottleneck from the consensus protocol to nodes’ processing capabilities. Conflux provides a decentralized and fully scalable blockchain platform that does not compromise security for its significant transaction speed improvements.