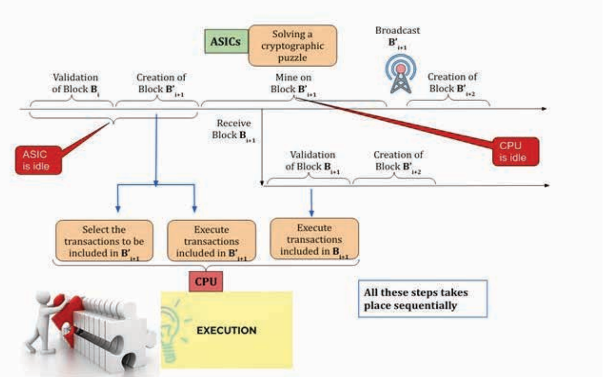
ASICs
Solving a cryptographic puzzle
Broadcast B'_{i+1}
Validation of Block B_i
Creation of Block B'_{i+1}
Mine on Block B'_{i+1}
Creation of Block B'_{i+2}
Receive Block B_{i+1}
ASIC is idle
CPU is idle
Validation of Block B_{i+1}
Creation of Block B'_{i+2}
Select the transactions to be included in B'_{i+1}
Execute transactions included in B'_{i+1}
Execute transactions included in B_{i+1}
CPU
EXECUTION
All these steps takes place sequentially

Maximising Computation in Blockchains

Problem Statement: Current Blockchain such as Ethereum allocates only a tiny fraction (e.g., less than 1% for Ethereum) of the average block inter-arrival time between blocks for validating smart contracts present in transactions. A trivial increase in the validation time introduces the popularly known Verifier's Dilemma, causes more forking and increases unfairness. Large validation time also reduces the tolerance for safety against a Byzantine adversary. Hence, Blockchains do not allow Computation Intensive Transactions (CIT). Solutions that offload validation to a set of non-chain nodes (a.k.a. off-chain approaches) suffer from trust and performance issues that are non-trivial to resolve. The current approach aims to allow the execution of CIT on the Blockchain without compromising security.

Uniqueness of the Solution: For the first time, this research has attempted an on-chain protocol to scale computation to 100% in PoW blockchains theoretically. The team has also pursued performing CPU-based block processing in parallel to ASIC mining. This is achieved by allowing miners to delay validation of transactions in a block by up to N blocks, where N is a system parameter. Researchers have developed a prototype implementation atop Ethereum, which demonstrates that it can scale without suffering the harmful effects of naïve scaling up of computation time in existing blockchains. Security analysis of this approach is also performed considering all possible adversarial strategies in a synchronous network with maximum end-to-end delay “D” and demonstrate that it achieves security equivalent to known results for longest chain PoW Nakamoto consensus.

Current Status of Technology: Prototype tested and security analysis performance is ongoing.

Societal Impact: Scaling computation on blockchain will allow integration of applications using heavy computation (including those using AI/ML, privacy-preserving cryptography etc.).

Patent(s): Filed

Relevant Industries: Blockchain, Software, Finance, Banking.

Faculty: Prof. Umesh Bellur, Prof. Vinay J. Ribeiro, Computer Science and Engineering.