HIGH THROUGHPUT DETERMINISTIC CONSENSUS THROUGH THRESHOLD SIGNATURES

A PREPRINT

Daniel J Guinan*
CTO, Vogsphere, Inc.
daniel.guinan@vogsphere.io
daniel.guinan@gmail.com

March 26, 2020

ABSTRACT

This paper introduces a family of high performance, leaderless, Byzantine fault tolerant protocols built around threshold signatures and deterministic concurrency in the form of a three stage computational pipeline that outputs a blockchain. These protocols provide deterministic, constant time and cryptographically non-repudiable consensus while simultaneously guaranteeing continued and correct processing in the presence of up to half of the network being Byzantine adversaries and/or failing nodes. Similar to traditional consensus protocols such as paxos, each consensus forming group, or *"consensus group"*, of nodes acts as a tightly coupled distributed computing cluster. But unlike traditional consensus protocols, they are decentralized, completely leaderless, with open joining and departure. The pipeline efficiently manages blocks of transactions at every stage, keeping up to three stages in-flight while messaging between nodes and the associated network traffic is constrained to only blockchain raw material, with any single node neither sending nor receiving more data to or from the network than will be contained in the next block in the blockchain.

Both permissioned and non-permissioned variants of the protocol are supported through a membership keychain, which is a derivative sub-chain of the blockchain. In the permissioned variant, nodes may only join if and only if their keys are accepted, whereas in the non-permissioned variant, nodes must provide a proof-of-capability and proof-of-stake, or equivalent, to be anonymously accepted and assigned into the membership keychain. The use of a keychain as a derivative of the blockchain allows cryptographic artifacts created through the consensus process to be rapidly verified without requiring the blockchain and provides proof-of-possession of participant keys, drastically simplifying cryptographic verification processes within the consensus machinery and by end users of the system. Through the use of this keychain, when deployed in a permissioned setting, these consensus protocols are suitable for deployment of decentralized public key infrastructure.

In this paper, we present the Vogon consensus protocol family, starting with a single instance of a consensus group working on a single blockchain. In later sections, we expand this into the general case of multiple consensus groups through the dynamic division and recombination of blockchain namespaces, generalizing the blockchain into a directed acyclic graph, and introducing a routing protocol loosely inspired by kademlia. Singular instances of Vogon consensus groups are particularly well suited for permissioned enterprise and coalition deployment while dynamic, non-permissioned, blockgraph deployments are ideal for global scale public decentralized infrastructure. When deployed in a permissionless setting, these consensus protocols manifest as a fully deterministic decentralized BFT network with massive throughput and hoizontally unbounded scalability.

***K*eywords** consensus group · membership keychain · proof-of-capability · blockgraph · horizontally unbounded

*Use footnote for providing further information about author (webpage, alternative address)—*not* for acknowledging funding agencies.