Introduction

The discussion of what a blockchain system is varies today in a heated debate. Without a doubt there is the blockchain data structure that everyone agrees is a linked data structure that utilizes prior hash values of prior data blocks or portions of prior data blocks to build its current state hash value. This chain of blocks maintains a complete history of the data structure that cannot be altered (the history) unless all of the hash values were re-computed. This data structure is then used with a distributed system where each node in the system maintains a copy of the data structure. Changes that are made to the data structure have to be done only when the system agrees a change is to be made. This process is often referred to as the consensus protocol of the system. The consensus protocol depends on the network infrastructure to facilitate the ability to communicate with participating nodes of the consensus system.

A consensus protocol can vary in centralization. A centralized type of consensus protocol can simply be a single point server that maintains consensus and when a new change is to be written to the data structure. A decentralized system is one in which the nodes independently work with each other in a well defined rule based approach where they either compete for the next change or vote for what is believed to be the next change. Many consensus protocols exist and early evidence tends to point to a general understanding that more centralization in the consensus protocol relates to higher performance while more decentralization relates to slower performance of the blockchain system. The general consensus is also that the consensus protocol is the greatest bottleneck in the blockchain systems.

Distributed blockchain systems are being developed and tested today to better understand the capabilities they provide. One aspect is becoming more apparent is that the level of integrity that these systems add is very desirable, especially in the systems that are the most decentralized. Many systems exist with varying levels of development to the platform including full graphical user interfaces to simply minimum interface server applications. Some are starting to be deployed in small prototypical test environments (simple small networks), some in parallel to existing systems, very few in full production.

Many reasons exist why full production of these types of systems are not very popular. The major reason is the technology has not reached full maturity. Researchers are still trying to narrow down the cost and benefits of the different types of systems. New systems are constantly being proposed faster than the research can be done to understand the good and the bad. Research for the most part is being done on individual systems to understand the performance of each platform. In these types of comparisons it is hard to understand weather the difference in performance is of the key technical features of the system or all of the other components implemented with the system.

Out of these new system implementations many unknowns still exist that needs to be better understood. For one many of these prototype systems exist only in small scale prototypes. Getting performance metrics on these test systems at scale can cost a lot of money and take a lot of time to test. Testing the systems at scale requires running many participating nodes on realistic networks. Setting these tests up can require large costs in computation resources and time for installation on resources. In particular all

of the different possible network configurations could have a large affect on the performance of these distributed systems, setting up the different networks would also have a cost for obtaining and setting up.

A test needs to be done so that a key feature of these systems can be appropriately compared in a more controlled scenario without the additional features implemented on top. The key feature that exists in all of the blockchain systems that contributes to the systems performance is the consensus protocol. Testing the consensus protocols themselves provides good benchmarks to what the different platforms can achieve. In the various platforms that utilize consensus protocols, features can always be modified to improve performance, but the protocol is a system that is core and is likely harder to improve other than changing the protocol used. Having a good understanding of the performance of the different protocols in different network topologies can help improve the decision making to what platform to use based on the core consensus protocol. What is needed is a system where the consensus protocols are interchangeable as well as the network that connects the system a system described in Figure 1.

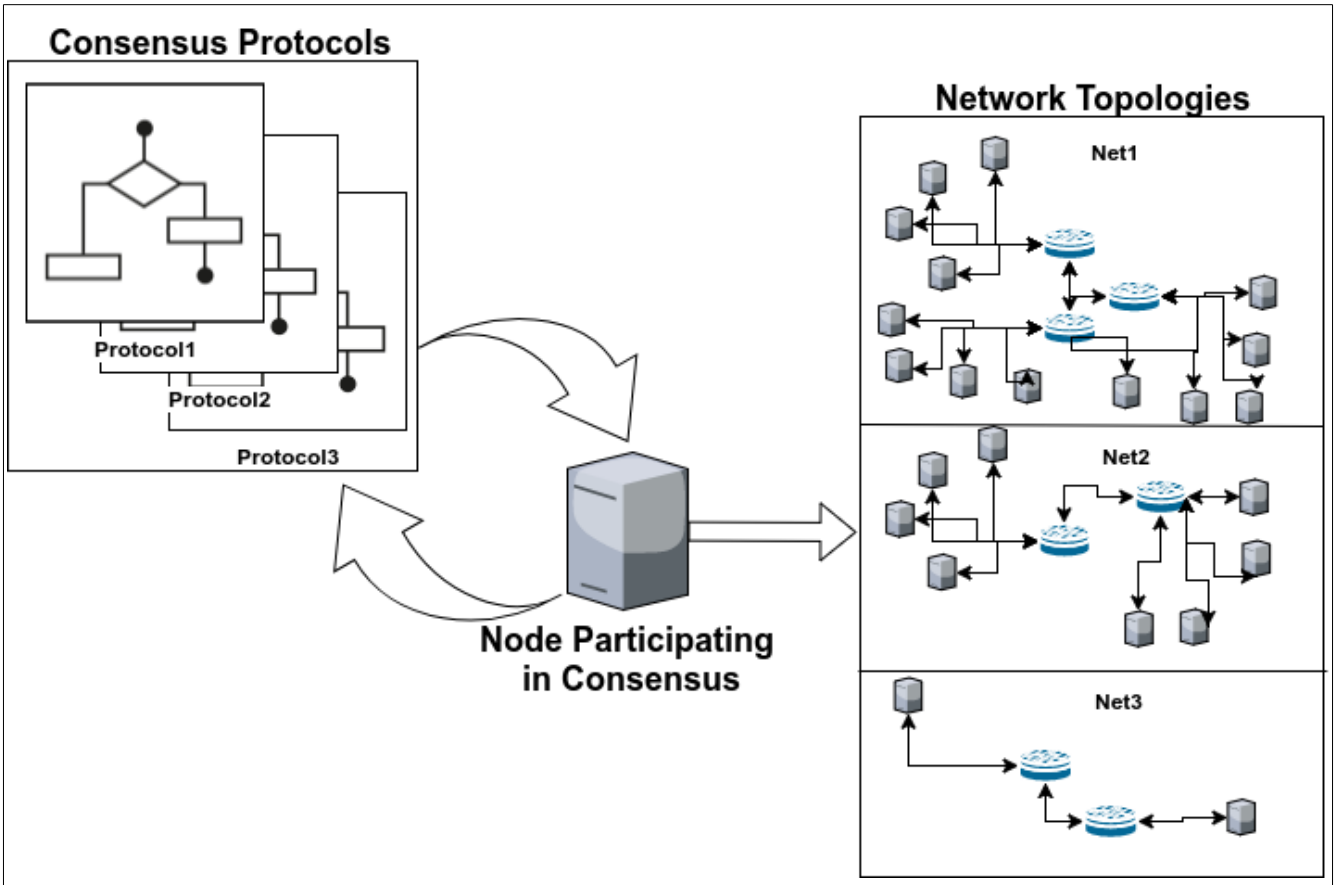

Figure 1: Ability to interchance the consenus protocol represented on participating nodes within different network topologies

A great way to test systems that might be expensive or require time to compute at scale is to utilize modeling and simulation (M&S). M&S utilize simplifications to represent the key aspects of the systems of interest in order to replicate the effects of the system with changes to the inputs, but in a fraction of time and a fraction of the cost. M&S is excellent at taking complex systems such as

distributed consensus systems and representing the effects of the feedback loops required by the nodes of the system. In particular the use of discrete event simulation where the simulation time step is system events rather than regular time steps allows for very fast computation. It achieves this by abstracting out and representing key aspects without actually implementing the entire system. For the blockchain based systems the key aspect that is of greatest interest in the consensus protocol. To model and simulate the performance of the many consensus protocols several tasks need to be accomplished.

1. The consensus protocols need to be generalized
2. The systems network needs to be modeled and able to be manipulated
3. The consensus protocol needs to be modeled to work with the modeled network
4. The complete model of the system needs to be simulated faster than real time so that many scenarios can be tested and performance of the system needs to be recorded

Accomplishing these 4 points will provide several benefits to the community over running many individual platforms with varying network setups. For one, the speed at which consensus protocols can be interchanged will create an environment where apples to apples tests can be done on all consensus protocols represented in the most rapid way possible. This approach will ensure that the key aspect to the blockchain systems performance is compared and not the efficiency of the platform itself. This is good in several ways. New platforms are designed and built constantly but a solid winner has not been defined so there is not a lot of certainty to what platforms will be the best in the future. The core protocols however will be used in not only the platforms of today but the platforms of the future.

This research will contribute to the benchmarking of the consensus protocols in different network topologies. The network defines the environment that these systems operate in. It is possible and the information would be of great use if it can be shown that certain consensus protocols perform better in certain environments. With this information developers will be able to better decide which consensus protocol would be preferred based on the environment for the system to be implemented in.

This paper describes how the consensus protocols were generalized and statistically represented in a discrete event model and simulation system. The model and simulation platform is built on an existing discrete event blockchain simulation built on network simulator (NS3). The authors will describe how the M&S system was calibrated, verified, and validated. Then example results are presented showing the capability of this approach.