Blockchain Consensus Algorithm - Proof Of DiGeST

Ramachandran Iyer

Abstract— In Blockchain world, arriving at a consensus over the correctness of a transaction is probably the most important and key element in the architecture of the blockchain framework. Dynamic consensus model help support various use-case and industry needs, based on the degree of decentralization and complexity needed. Consensus model is at the heart of any blockchain fabric and is very essential for managing and maintaining the decentral aspect of the solution.

Index Terms— Algorithm, Blockchain, Consensus, Dynamic, Proof-Of-Consensus

---

Dynamic Consensus

The dynamic consensus model, which will allow for starting with a default consensus model and allowing flexibility to switch to a different consensus model, based on either administrative option in private blockchain implementation and through a smart-contract voting mechanism built into the public blockchain system. Today the systems are very rigid and only allow for little option on the consensus model and even then you can only work with a single consensus model through the lifetime instance of the blockchain solution.

This will support multiple consensus model as an in-built option both in its public and private blockchain deployments and also an internal mechanism to trigger the change of a consensus model through a smart-contract trigger, which will be voted-on and based on broad agreement the switch to a new consensus will take place from the next block on.

Initially there will be support for dynamic consensus on the private side of the deployment model. On the public side there will be support for multiple consensus through side-chains and then at a subsequent major release support for dynamic pluggable consensus will be made on the public instance of blockchain.

Innovative New Consensus Algorithm : Proof Of DiGeST

Blockchain is at an very interesting point in time, where we are slowly but surely moving into real use-cases and starting to see result and value coming out from few 100's of PoC' that's happening around the world in both startups and large corporates. Blockchain is now gone beyond the realm of hype and getting into the phase of what I call " Rubber meeting the Road " phase, where things get to really get tested and starting to prove its mettle. That's the scene of where Blockchain is & the things that really power blockchain are a few key components and one of the most critical of them is the Consensus mechanism – which simply means how does the platform arrive at a consensus for validating whole bunch of user actions and gets committed to the block for eternity.

Consensus in Blockchain world is a critical and integral part to the decentralization philosophy that espouses to take the concentration of power and decision making from one core central entity to multitude of users, creating a democratic view of blockchain technology and how its positioned to change the way different products and solutions will be built over the next decade and beyond. One of the things we have been seeing in the way some of the public blockchain nodes exist got us thinking. For example the latest bitcoin node distribution shows ~44%+ of the Bitcoin blockchain nodes concentrated in only 2 countries (US Germany). This doesn't bode too well for a distributed story, where you'd like much more even distribution of nodes to ensure there is no regional grouping, clout that's formed or for nodes to aggregate easily given its general knowledge of where the concentration of nodes are. There is always a possibility of regional collusion which may destroy the fabric of consensus.

The Proof of DiGeST attempts to help solve that disparity by way of a new consensus algorithm. It's way of using geolocation and geodensity of nodes as key element of how the nodes are picked for candidature and eventually for the leader of the committee which commits the block. The idea is to give disproportional weightage for nodes which are actually farthest from the concentration geographies, who are benefited and given more change & power to participate in the block commits and balancing the natural tilt of favor and power in regional concentration geography nodes. So essentially the node selection is based on diversity and distributed the location in combination

with the amount of cryptographic tokens the user holds and a combined weightage to come to a selection of candidature for every round of COMMITTEE that's selected for ensuring the validation of transactions in a block. The leader is then elected from the committee. The elected LEADER of the COMMITTEE then commits the block to the blockchain platform. The framework also provides for a combination of Cryptographic randomness to be used for picking the LEADER of the COMMITTEE. It is also combined with the variability and option provided for the platform administrator who's setting up the blockchain to fine tune the parameters and configuration and change the levers at multiple levels either during the candidature of the COMMITTEE or during the election of the LEADER. This algorithm is a new idea which can be used by multiple blockchain protocol to implement a fast and next-generation protocol framework.

NODES

Nodes are any general purpose computer machines which register and become part of the Blockchain ecosystem. The Nodes can register by themselves if it's part of the public instance of the blockchain protocol or they will get invited if they are part of the permissioned instance of the blockchain system.

CANDIDATES

Candidates are nodes that form the Committee. Candidates are selected based on their geographic distribution, associated geographic density, associated cryptographic asset and associated reputation score.

LEADER

Leader are nodes that are elected automatically (software logic). In this case they are either elected through a cryptographic Lottery mechanism or as a randomized pick basis. The Leader once picked will be authorized and responsible for committing the block to the blockchain.

CRYPTO-ASSET

Crypto-Asset is the associated token that the user /node is ready to stake as part of the blockchain system. The crypto-asset forms one of the variable in the weighted scheme of things, when the leader is picked.

REPUTATION-SCORE

Reputation score of a node is built over a period of time and is based on multiple factors, which includes – node uptime, number of blocks validated, number of nodes listing node in black-list, holding time of crypto asset. The weightage on each cab be tweaked based of platform need and use-case.

Details of DiGeST

The proposed new consensus algorithm is a function of – Geographic Location, Geographic node density, Cryptographic asset holding of the node, Reputation score of the node. A combination of these which can be dynamically configured at the start of the platform deployment by a admin with a combined priority ranking of weightage can create a very dynamic flavor of the consensus protocol for each deployment of the system, which is very unique.

Differentiation

The uniqueness are largely based on three broad aspects. First being – it's a consensus mechanism in the blockchain technology space, where the nodes geographic location and geographic density is used a primary lever for score & weightage to be picked as a Candidate for the committee selection for the said block to be validated. The other uniqueness is about addition of other factors like holding of cryptographic asset value and reputation score, which is amalgamated dynamically to the primary lever while doing a weighted score. Another factor is about providing flexibility to administrators and giving them enough choices to fine-tune the consensus algorithm based on the need, use-case, type of blockchain, need for higher decentralization.

This will be an interesting mix of consensus model to the existing one's and one which will provide enough and more flexibility to administrators to move the various levers to either push for a broader and deeper consensus or to create a more light weigh consensus and allow for faster block time and hence the TPS rate. The blockchain space is evolving at a super pace and I'd reckon we will see existing models being challenged and newer models evolve as more use-cases hit real world deployment.

Figures and Tables

World Map Showing Bitcoin Node Density

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sun Sep 23 2018 21:33:49 GMT+0530 (India Standard Time).

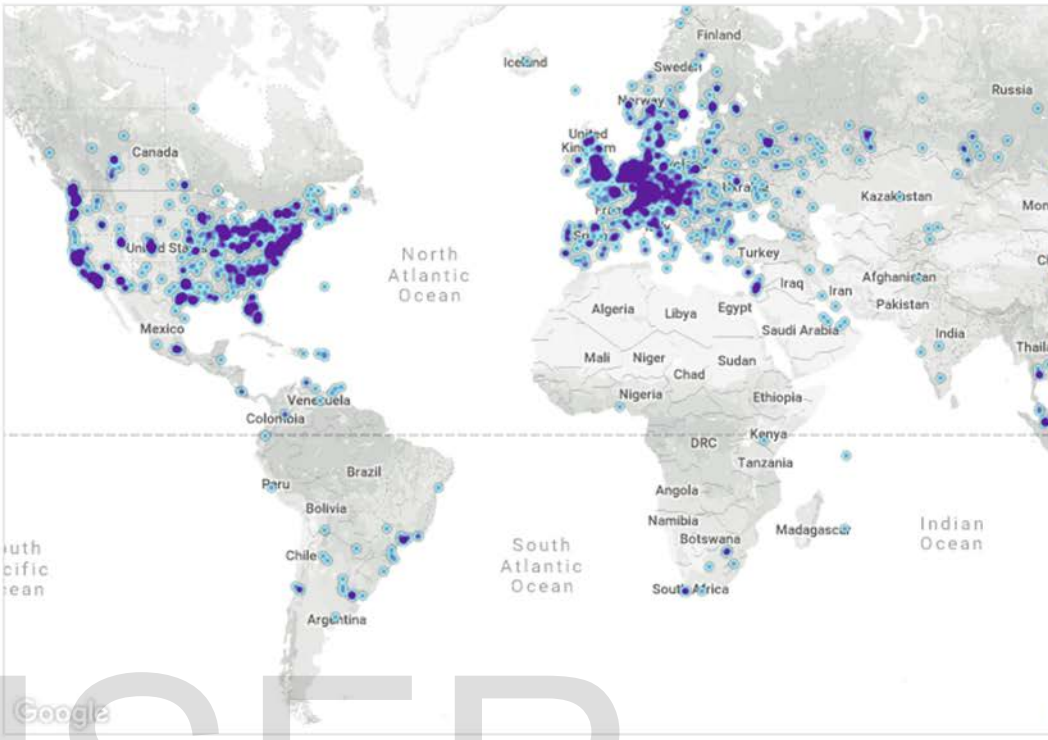
10089 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

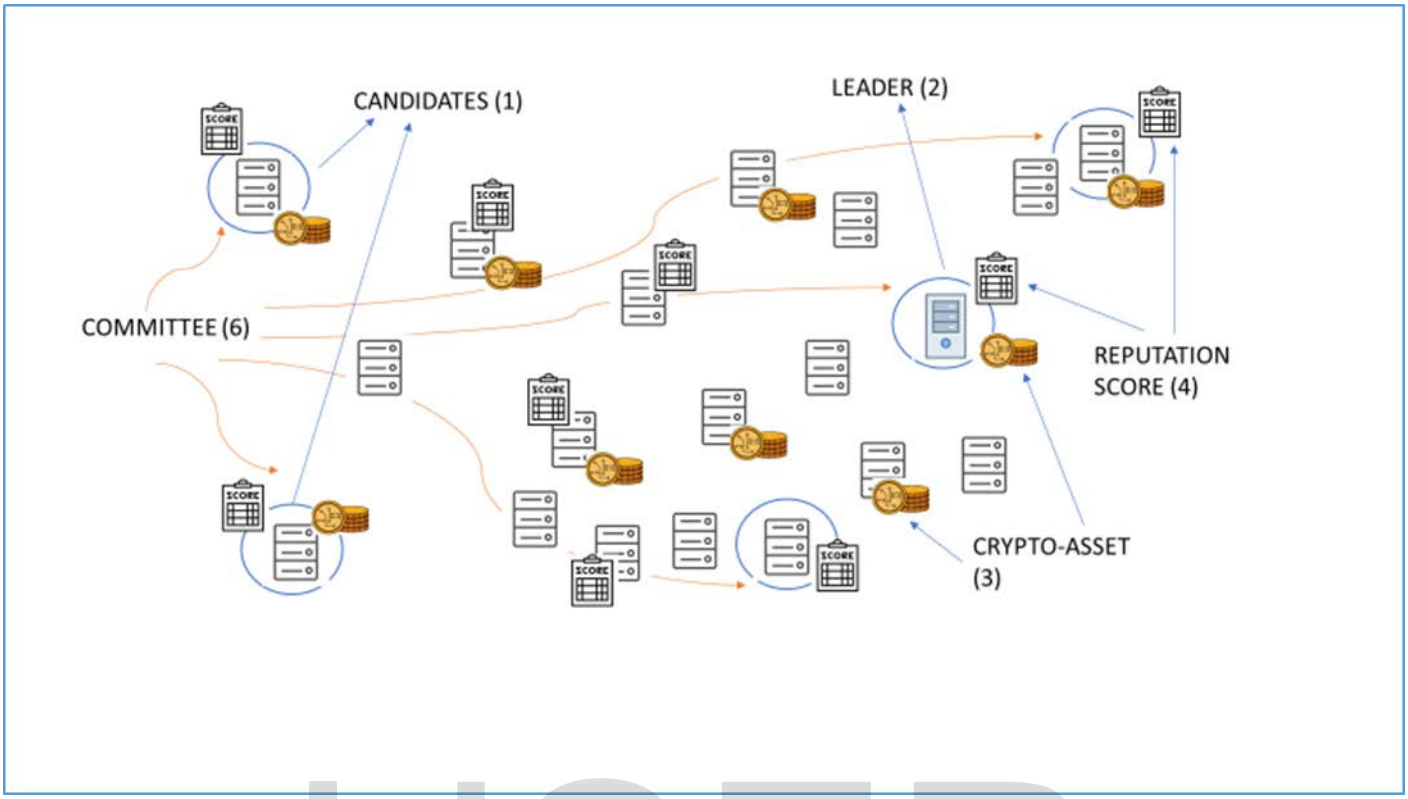
RANK	COUNTRY	NODES
1	United States	2385 (23.64%)
2	Germany	1941 (19.24%)
3	China	670 (6.64%)
4	France	667 (6.61%)
5	Netherlands	479 (4.75%)
6	n/a	461 (4.57%)
7	Canada	371 (3.68%)
8	United Kingdom	315 (3.12%)
9	Russian Federation	284 (2.81%)
10	Singapore	255 (2.53%)

More (99) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

Node Roles in Proof-Of-Digest



Conclusion

Proof Of DiGeSt will have enough flexibility for the administrator to expand or compress on various proof points and factors and make it either more heavy and decentralized with complex logic in lieu of lesser TPS or provide much light weight option on all of the factors to be able to achieve an extremely high TPS. Given this is a new & innovative consensus model, it will have full flexibility and control to make the needed happened and build this into the core protocol.