Discussion of Combining Distributed PoW Difficulty Over Multiple Block Chains For Equivalent Security of a Single Chain Block Chain

David Beberman
Prasaga, LLC

Author	Description	Version	Date
David Beberman	Initial Draft	0.1	03/01/19
David Beberman	Changed Hashpower estimate, removing blockrate normalization metric, and replaced with proportional estimate of blockrate / pow difficulty. Normalization does not give the desired result.	0.2	03/04/19
David Beberman	Typo fixes and added “disjoint” to describe union of groups of chains	0.3	03/07/19
David Beberman	Changed titles and wordsmithing as input for a PPA – updated version to 2.0 to distinguish from non-PPA work	2	04/02/19

Table of Contents

Discussion of Combining Distributed PoW Difficulty Over Multiple Block Chains For Equivalent Security of a Single Chain Block Chain

Abstract

The following text describes a consensus algorithm that is modeled on the blockchain longest chain algorithm. Although it is presented solely with respect to Proof-of-Work (PoW), it is expected to be combined with a version of Proof-of-Stake (PoS) as a complete consensus algorithm. Therefore this consensus algorithm, on its own, does not address all of the attack vectors that the combined consensus algorithm does. Describing this consensus algorithm independently forms the foundation for the combined PoS and PoW consensus algorithm.

Background to the Invention

Longest Chain Consensus

The longest chain consensus algorithm used by Bitcoin and others defines the longest chain as the valid or main chain. [provide reference]

Block Rate Production for PoW

The duration required to solve the PoW hash challenge for a given block is approximated by a function of two parameters: hashpower; and PoW difficulty, summed over all of the participating nodes.

Block rate $\approx \sum$ F (hashpower, PoW difficulty) – summed over all the nodes

The intent is that given two chains of blocks that link back to a common block, the longest chain is chosen as the correct chain by the participating nodes. The number of nodes is an unknown variable, but the length of each chain reflects indirectly the number of nodes, and thus the amount of resources expended on each chain. The consensus assumption is that the chain that has the most resources expended on it, is the correct chain.

If we make the following simplifying assumptions:

- The target block rate does not vary significantly over a localized time window
- The PoW difficulty does not vary significantly over a localized time window
- The hashpower for each node is approximately equivalent

then the longest chain reflects the most number of nodes performing PoW on that chain, implying the

greatest amount of resources expended on that chain. The largest number of nodes working on a chain is then the determining factor for the consensus.

If the hashpower for each node is allowed to vary, then the implication is there is a higher cost associated with a higher hashpower. The higher cost is then implicitly included in the resources expended on the longest chain. Although this implies that the longest chain may not have the largest number of nodes working on it instantaneously, the business social assumption that competition for the incentive rewards and transaction fees will encourage node operators to acquire equipment with competitive hashpower acts as a force towards approximately equivalent hashpower across all the nodes.

The longest chain consensus as described implicitly assumes that there is only one blockchain, and thus the objective is to converge on a single chain. If this implicit assumption is removed, and multiple chains are allowed, with some means for loose cooperation, the longest chain consensus can not be applied to such multiple chains as groups, where there may be a plethora of disjoint sets of chain groups. What is needed is a means to for the equivalent of a longest chain consensus among such a plethora of disjoint sets of chain groups. Therefore the following invention provides a means for a new consensus, suitable for choosing among a plethora of disjoint sets of chain groups.

Invention

The following is a brief description of the invention.

Distributed PoW Difficulty

Given a group of two or more blockchains and the following assumptions:

- Block rate production for each chain is approximately equivalent
- The PoW difficulty does not vary significantly over a localized time window
- The hashpower for each node is approximately equivalent
- A means to define the group of chains
- A means for the PoW hash solutions to be shared among the block chains

then the following:

- the total hashpower is the sum of the hashpower of all the nodes distributed across all the chains
- the PoW difficulty is the sum of the PoW difficulty distributed across all the chains.

Note that the specific PoW challenge for the blocks on each chain are local and independent for each chain.

The total amount of resources expended is the sum of the resources across all of the chains in the same manner as the single block chain approach.

Consensus Among Multiple Groups of Block Chains

The equivalent situation to the multiple chain consensus problem for a single block chain using PoW, is the multiple group of chains consensus problem for groups of chains.

The multiple group consensus problem is defined as the following:

- a means of grouping chains into subgroups which may or may not overlap with each other
- a means to share the PoW solutions between chains belonging to a group within that group.

then pick a single group that maximizes resources expended as the consensus group of block chains.

Solutions

Simplifying assumptions

- the block chains individual block production rates are approximately equal
- the PoW difficulty does not vary significantly over a localized time window for each block chain
- the hashpower for each node is approximately equivalent

then

- maximum disjoint unions of groups containing overlapping chains are derived (need correct set theory term here)

the largest disjoint union of groups implies the largest expenditure of resources and is the consensus group of chains. Chains that are not part of the largest union are not part of the consensus group.

Relaxing Common Block Rate Production Assumption

The block rate for a chain is determined by a function of the hashpower of the nodes and the PoW difficulty. For a given hashpower, block rate is inversely proportional the the PoW difficulty:

$$\text{Block Rate} \propto 1/\text{PoW difficulty}$$

Thus allowing for individual block chains to have different target block rates, with a given common hashpower, implies the PoW difficulty will vary for each chain with the target block rate.
Given that consensus is determined by the implied maximum expenditure of resources, the block rate and the PoW difficulty for a given block chain are not sufficient for determining expenditure of resources. Given two block chains:

Resource Expenditure 1 (Block Rate 1, PoW Difficulty 1, Hashpower) =
Resource Expenditure 2 (Block Rate 2, PoW Difficulty 2, Hashpower)

Provided Hashpower is common across the block chains, which include varying block rates, the consensus group remains the largest union of groups of overlapping chains. Therefore, varying block rate, and the resulting varying PoW Difficulty does not change the resource expenditure.

Relaxing Common Hashpower and Common Block Rate Assumptions

Allowing the hashpower for each chain to vary with respect to each other, and allowing the block rate for each chain to vary with respect to each other implies that the consensus group can not be determined based on the largest union of groups of overlapping chains, as a means to imply maximum resource expenditure. This can be seen as follows:

Block Rate $\propto$ Hashpower

Given two block chains:

Hashpower 1 >=< Hashpower 2

Block Rate 1 >=< Block Rate 2

PoW Difficulty 1 >=< PoW Difficulty 2

Then

Resource Expenditure 1 (Block Rate 1, PoW Difficulty 1, Hashpower 1) >=<
Resource Expenditure 2 (Block Rate 2, PoW Difficulty 2, Hashpower 2)

As a result, the maximum disjoint union of group of chains does not directly imply the maximum resource expenditure given the relaxed assumptions, which invalidates the group consensus algorithm based on solely on the maximum disjoint union of group of chains.

Relating Hashpower of Disjoint Groups of Blockchains

The hashpower of each chain is an unknown, but fixed over a localized time window quantity. The Block Rate is a known fixed quantity for each block chain. The PoW Difficulty relates the known Block Rate to the unknown hashpower. Block Rate can be written as the following:

Block Rate = F (PoW Difficulty, Hashpower)

Where F() maps values of PoW Difficulty and Hashpower to specific Block Rates. Further, Block Rate varies linearly with PoW Difficulty, which implies:

Block Rate / PoW Difficulty $\propto$ F(PoW Difficulty, Hashpower) / PoW Difficulty

This further implies that Block Rate / PoW Difficulty varies directly with varying Hashpower, which means that given two chains, with different Block Rates, that if:

Chain 1 Block Rate / PoW Difficulty > Chain 2 Block Rate / PoW Difficulty,

then

Chain 1 has more Hashpower.

Therefore:

Thus for each union of block chain groups the Union of Block Groups Resource Expenditure Estimate follows directly as:

Union of Block Chain Groups Resource Expenditure Estimate =
Σ Block Rate / PoW Difficulty

summed across all of the blockchains in each disjoint union of block chain groups.

The group of chains consensus is then:

group consensus = max (for all disjoint Union of Block Chain Groups Resource Expenditure Estimate).

Equivalence With Single Chain Maximum Resource Expenditure

The group of chains consensus represents the maximum resource expenditure of all union of block chain groups. As show above, total number of chains in the group of chains consensus may be less than another union of block chain groups, due to the allowance for varying block chain rates, and for implied varying of hashpower for each chain.

The single chain maximum resource expenditure consensus is defined to have a single non-varying block chain rate. Further, validation rules for most chains define that the rate of change of PoW Difficulty is locally insignificant across multiple blocks in the block chain. Therefore, given the assumptions and derivations above:

Resource Expenditure Estimate $\propto$ Block Chain Length

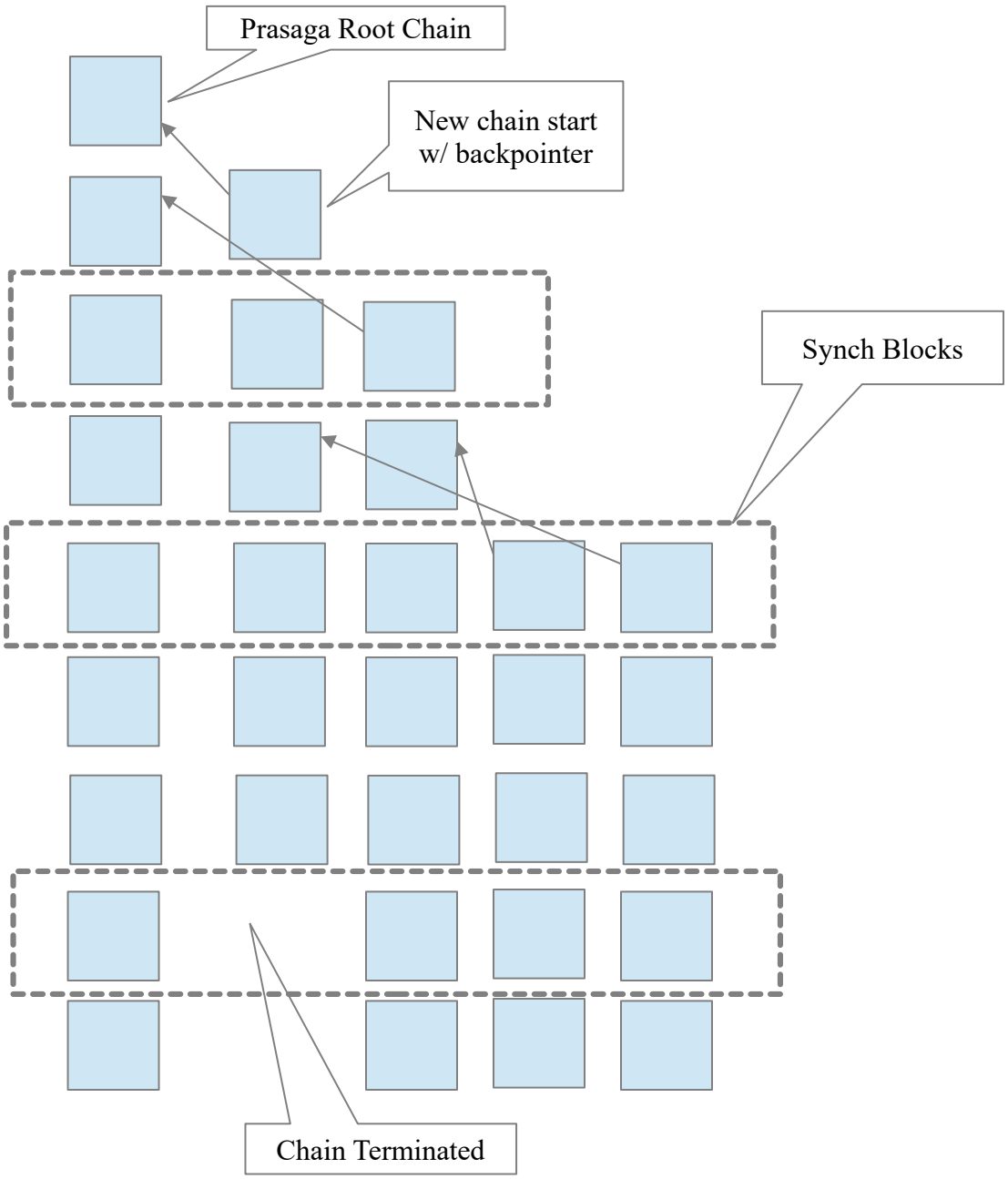
and

max length (for all Block Chains) $\propto$max (for all resource expenditure estimates)

Thus maximum block chain consensus algorithm for a single chain, implies choosing the maximum

resource expenditure estimate, in the same manner as the group of chains consensus.

Multiple Block Chain diagrams



Synch Block

As depicted above, the current PoW solution for each chain is shared with all other chains periodically. The PoW solutions are included in each chain creating a common list of PoW solutions over all the chains. Each block with the list of PoW solutions is termed a synch block.

The inclusion of the synch block in each chain, enables the following validation rule:

- The PoW solution for every other chain contained in a given chain's block chain, must exactly match the PoW solution of the block of the original chain source

The resource expenditure estimation is applied to all of the block chains identified in the synch block and that pass validation. Any block chains that do not pass validation are eliminated, before resource expenditure estimation.

Each synch block is defined as identifying a group of chains.

Maximum Union of Overlapping Group of Chains

The maximum union of overlapping group of chains is defined as the union of all chains identified in one or more synch blocks within a given time window, such that each synch block shares at least one chain with at least one other synch block in the given time window. Chains are only considered if they pass all validation rules.

Groups of Disjoint Union of Chains

The usual case is that the maximum union of overlapping group of chains is equal to the total number of chains, with the exception of invalid chains. This is equivalent to the main chain consensus for single chains.

Disjoint unions given the synch blocks may occur due to network partitioning events, attackers, or other anomalies. Such events are similar in concept to the forks that the single chains experience from time to time. The normalized resource expenditure estimate is performed for each of the disjoint union of group of chains, defined by the synch blocks. The maximum resource expenditure rule defines the group of chains consensus.

Further Considerations

Attack Considerations

The primary concern for an attack is to fork a block chain to enable a doublespend. Other forms of attack such as denial-of-service are not considered with respect to the group of chains consensus algorithm.

Transaction Confirmation

The receiver of a transaction determines the acceptance of a transaction after both several confirmations on the blockchain that contains the transaction have occurred, and one or more synch blocks have also been confirmed on that blockchain.

Doublespend Attack

By definition, the amount of hashpower for any given individual chain is only a fraction of the total hashpower distributed across all the block chains. Therefore the hashpower that an attacker needs to mobilize for a 51% or greater attack is far less than a similar attack on a single chain. The attacker thus is able to fork an individual chain with sufficient hashpower. The attacker would then attempt to create an alternative chain which enables the opportunity for doublespends.

However, due to the sharing of PoW solutions across all the other chains, to fork the chain post a synch block, the attacker would need to modify the PoW solution recorded in the synch block across all other chains included in the group of chains consensus. This effectively forces the attacker to need 51% of the total hashpower across all the chains.

Conclusion

The maximum resource expenditure estimate applied to the maximum disjoint union of groups of chains, enabled with the periodic sharing of PoW solutions across all of the chains, is an equivalent consensus algorithm as the PoW longest chain algorithm used by current single chain block chain designs typified by Bitcoin.

The group of chains consensus algorithm is not sufficient, on its own, to protect against all of the attacks that the PoW longest chain algorithm for single chain block chains is able to. Instead, the intent of the group of chains consensus algorithm is to combine it with a proof-of-stake consensus algorithm and additional validation rules to create a combined PoW and PoS consensus that is at least as secure as the PoW longest chain consensus algorithm, and believed to be stronger than any PoS consensus algorithm.