Simple Extended Consensus Resolution: Uncle Mining On The Blockchain

Thaer Khawaja
thaer.khawaja@gmail.com
www.getmasari.org

Abstract

Since Bitcoin's inception and introduction of cryptocurrency[1], alternative iterations of permissionless decentralized peer-to-peer electronic cash have been developed. However, most of these systems have the same blockchain properties that subsequently retain similar on-chain scalability limitations to Bitcoin. With the introduction of the SECOR protocol, we propose a simple version of Uncle Mining, serving the purpose of faster block emission rates while further securing the network by rewarding miners for otherwise-orphaned blocks, solving in part some of the inherent scalability limitations of blockchain technology. These added properties are achieved by introducing block weight and differentiating it from block difficulty in a hash-based proof-of-work (PoW) system that achieves consensus via the heaviest chain in the network.

1 Introduction

Since the introduction of Bitcoin, the scalability of permissionless decentralized cryptocurrency systems has been put into question, with different on-chain and off-chain solution proposals introduced in the space. When looking at on-chain scalability protocols, block emission rates become very important as they're necessary for consensus. If blocks are emitted too fast, the network will not be able to converge on the state of the network. Conversely, if blocks are emitted too slowly, the network is slow to update state and at scale would have the problem of very large blocks congesting the payloads being broadcasted; at some point the blocks become too big for consensus when propagation times exceed that of a given emission rate. To help with on-chain scalability, a protocol such as SECOR is needed for achieving an optimal emission rate with security measures in place to maintain consensus. When implemented, it would in turn deliver faster blocks and higher network security as it takes advantage of what would otherwise be stale orphaned blocks not accepted into the network.

2 Simple Extended Consensus Resolution (SECOR)

We define the blockchain as a directed acyclic graph $G = (V, E)$, containing the active main chain and the set of all alternative chains. The main chain corresponds to the max weighted path from the genesis block v_0 to the latest block at v_h, with h representing the current chain height at the max weighted path of G, $W = \sum_{i=0}^{h} weight(v_i)$. The weight of a block v_i corresponds to the computed difficulty for mining it plus the difficulty of a mined uncle. An uncle mined on the main chain is an alternative block v_{h-1}^{a} with a sibling v_{h-1}^{m} on the main chain, $a \neq m$, distinct solutions at height $h-1$, and a nephew block ${}_{m}^{a}v_{h}^{n}$ is referencing the uncle a with its parent m (notation: ${}_{parent}^{uncle}v_{height}^{current\_block}$).

2.1 Properties of a Valid SECOR Uncle

2.1.1 Common Ancestry

At least one of these two cases must be present for a valid uncle.

Direct Ancestry. The grandparent v_{h-2}^{γ} of candidate nephew block v_h must be the same direct ancestry reference in parent v_{h-1}^{m} and uncle v_{h-1}^{a}.

Extended Ancestry. This scenario is allowed at $h+1$ when there are two candidate top blocks ${}^{a}_{m}v^{i}_{h}$ and ${}^{m}_{a}v^{j}_{h}$, $i \neq j$, where the parent of v^i is the uncle v^j, the parent of v^j is the uncle of v^i, and the grandparent γ is the same direct ancestry of those two blocks. This double reference ensures these are publicly known alternative paths, and by direct ancestry to grandparent γ it ensures this uncle mining case for the active main chain is publicly known.

2.1.2 Correct Uncle Reference

The computed hash that represents new top nephew block ${}^{a}_{m}v^{n}_{h}$ must include in it the hash of uncle $hash(v^{a}_{h-1})$ to ensure that the reward given to to the uncle is valid relative to its coinbase output. The uncle coinbase reward r^a must be a defined constant fraction of the original amount in order to disincentivize adversarial uncle mining, and a fraction must be rewarded to the nephew reward r^n.

2.1.3 Near Time Constraint

In order to avoid any potential time warp attacks in the set of timestamps, the uncle block's timestamp t_a must be a defined delta from the parent timestamp t_m that is reasonable relative to block propagation statistics - this assumes the clock drift in nodes of the network are minimal, and is only to be enforced with a supporting block emission rate T (i.e. the delta with for T = 60 could be be $|t_a - t_m| < T/4$ which is sufficient given block propagation delays).

3 Features of a SECOR Enabled Network

3.1 Faster Block Emission Rates.

3.1.1 15 Second Blocks.

This is constrained by hardware limitations, and we can use Bitcoin as reference on network block propagation performance, where each KB costs an additional 80ms delay until the majority knows about the block, with 95% of nodes have observed the broadcast within 40 seconds, and an overall mean of 12.6 [2]. More recent Bitcoin statistics give improved and converging results, with a 50th percentile (p50) mean of 3.7 seconds, p90 mean of 17.5, p90 median of 15.7, and a max p90 value of 48.5, when looking at recent data with saturated blocks (2016-04-05, 2017-04-05) [3]. Therefore, when controlling block size and compute costs, it's arguable that block emission rates as low as 15 seconds are sufficient for consensus, with SECOR as a protection measure against outliers and adversaries.

3.1.2 Smaller Blocks.

This is important with projects such as those using the CryptoNote protocol providing dynamically adjustable block sizes, where there is a larger constant associated with the transactions proofs involved [4]. SECOR's ability to safely increase block emission rates helps with propagation as it would introduce less latency into the system. There is a balance, however, as too fast of an emission rate can introduce many empty blocks where their coinbase transactions could help with statistically significant analysis on traceability of normal transactions.

3.2 Improved Network Security.

3.2.1 Heaviest Chain Consensus.

While consensus in a traditional PoW system is based off the greatest PoW effort invested, with cumulative difficulty $D = \sum_{i=0}^{h} difficulty(v_i)$ determining the active chain in the network, using the cumulative weight W enables miners to effectively double the difficulty of a block every time an uncle is mined, resulting in $W \geq D$. Considering a rational adversary intentionally mining uncles, one is disincentivized as long as the uncle reward for doing so is less than mining sequential blocks, therefore any intentional uncle mining would be less profitable than mining on the main chain. With near-time uncle timestamp constraints, the difficulty computed from these alternative blocks would be very similar and any secretive mining following

those produced blocks is reducible to adversarially mining two hidden subchains, which falls under the same exponentially decreasing probability of an attacker catching up as previously made analogous to the Gambler's Ruin problem[1].

3.2.2 Uncle Rewards.

Rewarding miners for otherwise-orphaned blocks, incentivizes miners to participate in the protocol while at the same not biasing high performance network connections, and not significantly punishing those collaborating with low performing hardware.

4 Additional Related Work

The implementation of this protocol has been completed in the Masari Project, a CryptoNote based coin. Initial inspiration of this protocol was from the GHOST and DECOR protocols, where their main focus differed slightly from SECOR's due to seeking for consensus using emission rates nearing or faster than hardware limitations, needing to account for multiple uncles at a given height and the efficiency rates of a network implementing it[5][6][7]. With the introduction of SECOR, the distinction is simplicity due to future research that looks to further increase throughput without needing to optimize past hardware limitations.

5 Conclusion

This paper presented SECOR, a simple uncle mining protocol which can deliver fast block emission rates and higher network security, optimizing propagation rates with smaller higher frequency blocks. The tight coupling of uncle references within the chain and only allowing a single uncle reference per block limits adversarial attacks as they become synonymously equivalent to 51% attacks. The distinction of weight from difficulty allows separation of difficulty calculation in adjustment algorithms, from cumulative weight that would otherwise determine the active main chain.

Additional research is needed to further optimize mining by partitioning the main chain into dynamically adjustable shards, where the block tree of alternative chains is distinct from the block tree of active main sub-chains, redefining the Blockchain as the Blocktree. This future work would further split individual block difficulty into smaller units, bypassing the converging hardware limit on block emission rates, and allowing one to set a maximum block size without worry of network congestion or high transaction fees. This has the advantage of further improving block propagation throughput, and increasing decentralization of compute due to smaller mining pools being able to more consistently mine blocks and incentivize miners away from the bigger pools. Related work would include PoW supplementary algorithms that bind mining to forced I/O operations using a dynamically scalable and large enough scratch pad that cannot be optimized into memory, an eco-friendly approach to exponentially decreasing the amount of compute necessary to secure the network, leveling the playing field between CPUs and ASICs. Given such a high transaction throughput & low latency proposal as Blocktree, with a high security & low compute PoW algorithm, the permissionless decentralized cryptocurrency model could in the future rival centralized networks such as VISA.

References

[1] Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System.* bitcoin.org/bitcoin.pdf (2008)

[2] Decker, Christian., Wattenhofer, Roger. *Information Propagation in the Bitcoin Network.* tik.ee.ethz.ch/file/49318d3f56c1d525aabf7fda78b23fc0/P2P2013_041.pdf (2013)

[3] BitcoinStats. *Data Propagation, 2013-11-22 to 2017-04-05.* bitcoinstats.com/network/propagation/

[4] Saberhagen, Nicolas. *CryptoNote v 2.0* https://cryptonote.org/whitepaper.pdf (2013)

[5] Sompolinsky, Y., Zohar, A. *Secure High-Rate Transaction Processing in Bitcoin.* eprint.iacr.org/2013/881.pdf (2015)

[6] SDLerner. *Even faster block-chains with DECOR protocol.* bitslog.wordpress.com/2014/05/02/decor/ (2014)

[7] Ethereum, Blog. *More uncle statistics.* blog.ethereum.org/2015/09/25/more-uncle-statistics/ (2015)