Prunality of the GHOSTDAG Protocol

Michael Sutton, Shai Wyborski

July 2020

1 Introduction

This document details a set of rules miners in the GHOSTDAG [1] protocol must follow in order to support secure pruning of the DAG.

2 Notation and Rules

Parameters:

- ϕ – Finality depth
- k – PHANTOM parameter
- ℓ – Merge bound
- $\pi = 2\phi + 4\ell k + 2k + 2$ – Pruning depth

Definition 1. Some notations:

- $\overline{P}ast, \overline{F}uture, \overline{C}hain$ are the inclusive counterparts of $Past, Future, Chain$
- $B.Subtree = \{C : \quad B \in C.Chain\}$
- $B.MergeSet = B.Past \setminus B.SelectedParent.\overline{P}ast$
- A block B is said to be a *merging block* of block Y, if $Y \in B.MergeSet$.

Definition 2. For any integer n and any block B let

$$B_n = \text{argmax}_{C \in B.Chain}\{w(C) < w(B) - n\};$$

We name some useful blocks:

- The block at *depth* n is Virtual_n
- The *finality block* is $F = \text{Virtual}_\phi$
- The *pruning block* is $P = \text{Virtual}_\pi$

Corollary 1. *For any integer n and any block B*

$$w\big(B\big) - n - k - 1 \leq w\big(B_n\big) < w\big(B\big) - n;$$

Proof. The second inequality follows directly from Definition 2. The first follows from maximality of B_n. Assume $w\big(B_n\big) < w\big(B\big) - n - k - 1$. Since each chain block can add at most $k+1$ blue blocks, their must exist a block $C \in B.Chain$ where $C.SelectedParent = B_n$, and which satisfies $w\big(C\big) < w\big(B\big) - n$. Contradicting maximality of B_n. □

Corollary 2. *For any block B and any integers m, n s.t. $m > n$*

$$w\big(B_m\big) < w\big(B_n\big) + n + k + 1 - m;$$

Proof. This is a direct result of applying Corollary 1 over B, m and obtaining $w\big(B_m\big) < w\big(B\big) - m$, applying the same corollary over B, n and obtaining $w\big(B\big) - n - k - 1 \leq w\big(B_n\big)$, and combining the inequalities. □

Definition 3 (Pruning invalidation rules)**.** A block B is considered invalid if one of the following holds:

(R-I) (Objective finality)

$$\begin{aligned}\exists Y \in B.MergeSet \cap B_\phi.Anticone :& \\ & Y.Future \cap B.Blues \cap B_\phi.Subtree = \emptyset\end{aligned}$$

(R-II) (Bounded merge)

$$|B.MergeSet| > \ell$$

(R-III) (Blood exile)

$$\exists C \in B.Parents : \quad C \text{ is invalid}$$

Assumption 1. There is no 51% attacker and ϕ was chosen so that (malicious or organic) splits of depth ϕ have negligible probability. We consider them as impossible.

3 Main Proposition

Proposition 1. *If when B was discovered it held that $B \notin P.Future$ then B will never be in the past of Virtual.*

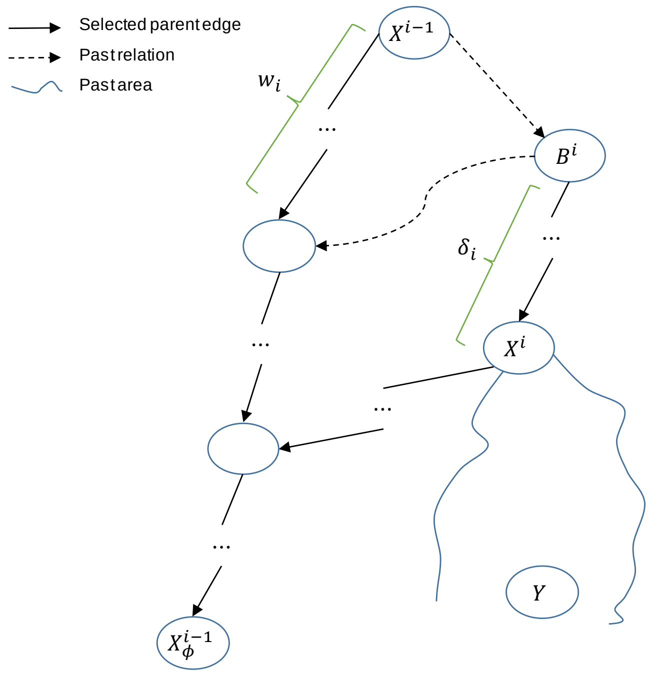

Figure 1: Illustration of induction variables.

Proof. Let Y be a block which, when it was discovered, was not in $P.Future$. Assume that at some future point in time Y was in Virtual.$Past$. Let $X \in$ Virtual.$Past$ be minimal such that $F \in X.Chain$ and $Y \in X.Past$, such an X must exist by hypothesis and Assumption 1 (though it may not be unique).

We now define a sequence of merging blocks $X = X^0, \ldots, X^m$, in the following way:

- Given X^{i-1}, select a block $B^i \in Y.Future \cap X^{i-1}.Blues \cap X_\phi^{i-1}.Subtree$. Such a block must exist by induction hypothesis.
- Select X^i to be a block $\in B^i.\overline{C}hain$ s.t. $Y \in X^i.MergeSet$. Such a block must be unique if it exists. See Figure 1 for an illustration.
- If no such merging block exists, set $m = i - 1$ and halt the process. This can only happen if $Y \in B^i.Chain$.

We now define counting measures for the process. Let $w_i = w\big(X^{i-1}\big) - w\big(\max X^{i-1}.Chain \cap B^i.Past\big)$; and denote $\delta_i = |B^i.Chain \setminus X^i.Chain|$. Note that w_0, δ_0 are undefined and that $\delta_i = 0$ *iff* $B^i = X^i$. See Figure 1.

Claim 1.

$$\forall i \in [1, \ldots, m] : \quad w_i \leq 4k + 1$$

Proof. This follows from blueness of B^i and from an argument similar to that of GHOSTDAG's [1] freeloader bound (B^i being a block freeloaded by X^{i-1}). $\square$

Claim 2.

$$m + \sum_{i=1}^{m} \delta_i < \ell$$

Proof. Let Δ_i denote the set $B^i.\overline{C}hain \setminus X^i.Chain$. It needs to be shown that $\forall i \in [1, \ldots, m], \Delta_i$ are disjoint subsets of $X.MergeSet \setminus \{Y\}$ which has size $< \ell$ by (R-II).

The subset property follows easily from the fact that all blocks in Δ_i are in $Y.Future \cap X.Past$. Assume that there exists a block $B \in Y.Future \cap X.Past, \notin X.MergeSet$, so $B, Y \in X.SelectedParent.Past$ which contradicts minimality of X. The disjoint property follows directly from the inductive selection process. Noting that $|\Delta_i| = \delta_i + 1$ gives the desired result. $\square$

Claim 3.

$$w\big(X^m\big) > w\big(F\big) - 4\ell k$$

Proof. By definition of w_i we have that $w\big(X^{i-1}\big) - w_i < w\big(B^i\big)$. Additionally, noting that $X^i \in B^i.\overline{C}hain$ and that each chain block can add at most $k+1$ blue blocks, we get that $w\big(B^i\big) \leq w\big(X^i\big) + \delta_i\big(k+1\big)$.

Reorganizing terms, we obtain a bound on the score distance between two consecutive merging blocks

$$w\big(X^{i-1}\big) - w\big(X^i\big) < w_i + \delta_i\big(k+1\big);$$

Summing up this inequality over $i = 1, \ldots, m$ and using Claims 1, 2, we get $w\big(X^0\big) - w\big(X^m\big) < m4k + \sum_{i=1}^{m} \delta_i(k+1) \leq 4\ell k$, where the last inequality holds since $k > 0$. The desired result follows since $F \in X^0.Past$, so $w\big(F\big) < w\big(X^0\big)$. $\square$

Claim 4.

$$\forall i \in [0, \ldots, m]: \quad P \in X^i_\phi.Chain$$

Proof. By induction on i.

Basis: For $i = 0, X = X^0$, the claim follows immediately since $P, X_\phi \in X.Chain$ and $w\big(X_\phi\big) > w\big(P\big)$.

Inductive step: Assume that $P \in X^{i-1}_\phi.Chain$. We will now show that $P \in X^i_\phi.Chain$. By definition of B^i we have that $X^{i-1}_\phi \in B^i.Chain$. The selection process also implies that $X^i_\phi, X^i \in B^i.Chain$. Combining with the induction hypothesis we get that $P, X^i_\phi \in B^i.Chain$. Since both blocks share a chain, it remains to show that $w\big(P\big) < w\big(X^i_\phi\big)$. Following Claim 3 and noting that $X^m \in X^i.Past$, we get that $w\big(X^i\big) > w\big(F\big) - 4\ell k$. Combining with Corollary 1 over X^i, ϕ we have

$$w\big(X^i_\phi\big) > w\big(F\big) - 4\ell k - \phi - k - 1.$$

On the other hand, by plugging Virtual, π, ϕ into Corollary 2, we get that

$$w\big(P\big) < w\big(F\big) - 4\ell k - \phi - k - 1;$$

so $w\big(P\big) < w\big(X^i_\phi\big)$.

$\square$

Conclusion: From Claim 4 it follows that $\forall i \in [0, \ldots, m], Y \in X^i_\phi.Anticone$. To see this, note that $Y \in X^i_\phi.Future$ would imply that $Y \in P.Future$, which is a contradiction, and that $Y \in X^i_\phi.Past$ contradicts $Y \in X^i.MergeSet$. This justifies the induction hypothesis that B^{i+1} must exist $\forall i \in [0, \ldots, m]$, otherwise violating (R-I), (R-III). Specifically, it must be assumed that $B^{m+1} \neq Y$ exists, where by definition $X^m_\phi \in B^{m+1}.Chain$. However by halting of the process it follows that $Y \in B^{m+1}.Chain$. Since $Y \in X^m_\phi.Anticone$, Y, X^m_ϕ cannot share a chain, thus leading to a contradiction.

$\square$

From this follows that it is secure to implement the following:

Rule 1.

- All blocks in $P.Past$ can be pruned, and
- For block B, if it holds that $B \notin P.Future$ and $B \notin$ Virtual.$Past$ (that is, B violates finality rules of Virtual), then B can be discarded

References

[1] Yonatan Sompolinsky, Shai Wyborski, and Aviv Zohar. PHANTOM and GHOSTDAG: A scalable generalization of nakamoto consensus. Cryptology ePrint Archive, Report 2018/104, 2018. `https://eprint.iacr.org/2018/104`.