Consensus and Security in Canonchain

Lei Zhang[*]

November 7, 2019 Version 2.1

Abstract

In this paper, we build up the mathematical foundations of Canonchain, which utilizes directed acyclic graph (DAG) for storing transactions. We provide thorough and rigorous analysis on our consensus mechanism which depends on non-anonymous reputable entities, called witnesses. Our scheme allows witnesses to be replaced to achieve higher level of decentralization. The security of Canonchain network against malicious behaviors is guaranteed.

1 Introduction

The concept of blockchain as an independent technology began to surge in 2015. Prior to this, it was known as the data structure of Bitcoin. In Nakamoto's white paper [1], the two words "block" and "chain" appear together, but it only refers to "a series of blocks." With the popularity of Bitcoin, the technology and concepts in Bitcoin is often classified as Blockchain 1.0. With Ethereum [2] running as a platform for distributed applications, people began to classify Ethereum as Blockchain 2.0. Now the market is vying for the fundamental structure for a new paradigm of Internet infrastructure, interoperability and scalability, i.e., Blockchain 3.0. Many people think that directed acyclic graph (DAG) structure is one of the best candidates.

In traditional blockchain technology represented by Bitcoin and Ethereum, blocks and transactions are two separate concepts. A transaction is confirmed by the miners and packed into a block, and the throughput in terms of transactions per second (TPS) is limited by the block size and the block generation speed. In addition, miners in the blockchain system have the right

[*]Author's contact information: leizha@ntlabs.io

to decide the content of the block. The profit-seeking behavior of the miners can easily lead to excessive concentration of power or voting rights, thus losing the decentralization characteristics. DAG-based distributed ledger technology (DLT) was created to solve these problems. Compared to traditional blockchain technology, DAG-based DLT has the following advantages: 1) Strong scalability (high TPS); 2) Fast transaction speed; 3) (Almost) no transaction fee and friendly to small payments; 3) No requirement for special miners to participate.

The idea of using DAGs in the cryptocurrency space has been around for a while. DAGLabs has proposed a series of consensus protocols, such as Inclusive [3], SPECTRE [4] and PHANTOM [5]. The general idea behind them is to utilize a DAG of blocks. Also the miners in the system still compete for transaction fees, and new tokens may be created by these miners. Instead, some cryptocurrencies depend on a DAG of individual transactions other than blocks. IOTA [6] and Byteball[1] [7] are among the oldest and most representative projects. They both have the same advantages using a DAG structure, but have quite different design details in order to cater to different audiences. IOTA assigns a certain weight to each transaction, and the transaction is generated through the proof of work (PoW) mechanism. Instead of utilizing PoW, Byteball prevents junk transactions by charging a small fee, and introduces votes from witnesses to determine valid transactions.

Similar to IOTA and Byteball, transactions in Canonchain are stored and organized in a DAG structure. However, we impose some additional rules, which results in a special DAG called regularized directed acyclic graph (R-DAG). Consensus in our R-DAG is achieved through witnesses, which are non-anonymous reputable entities. It is a Byzantine Fault Tolerant (BFT) consensus protocol which can tolerate malicious behaviors. Since the FLP impossibility result [8] has demonstrated the impossibility of distributed consensus in an asynchronous environment, we assume one of the two forms of partial synchrony defined in [9]. That is, the upper bound on the time required for a message to be delivered is fixed but not known a priori. The main advantage of our consensus algorithm, compared with the state-of-the-art BFT protocols such as PBFT [10] and Tendermint [11], is the exclusion of additional messages for voting purpose. It significantly reduces the communication overhead, which in turn alleviates the scaling issues to achieve higher TPS.

The remainder of the paper is organized as follows. Cannonchain R-

[1] Byteball project has been renamed as Obyte.

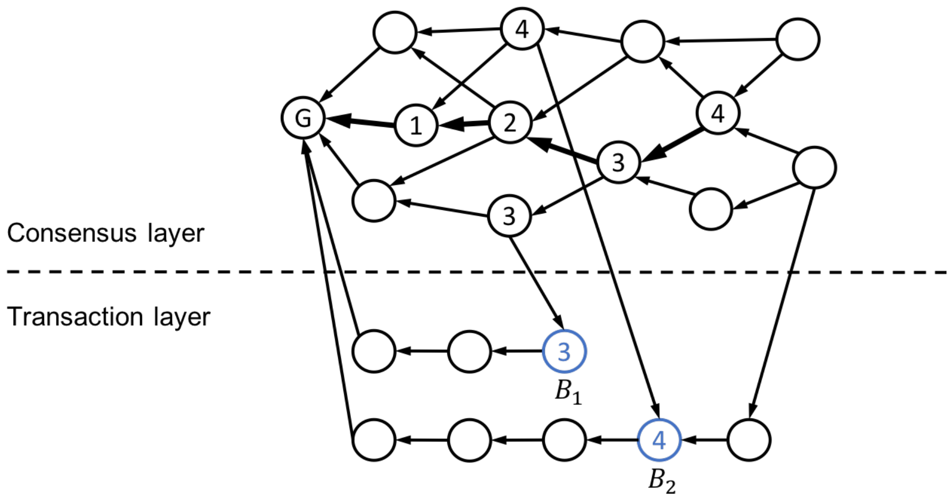

Figure 1: Example of consensus in R-DAG structure

DAG structure is presented in Section 2. The proposed consensus algorithm is described in Section 3. Section 4 rigorously proves the correctness of our consensus protocol, including both safety and liveness properties.

2 R-DAG

In Canonchain, each block represents one transaction, which contains references to previous blocks (called parents) through their hashes. Blocks and their parent-child links are the vertices and edges of the DAG, respectively. As depicted in Fig. 1, our R-DAG structure has two layers, namely the consensus layer and the transaction layer.

All blocks in the consensus layer are composed by some non-anonymous reputable people or companies, called witnesses, who might have a long established reputation, or great benefits in keeping the network healthy. Each block in the consensus layer can reference multiple blocks from both the consensus layer and the transaction layer. Witnesses are expected to post transactions frequently and behave honestly. However, it is unreasonable to totally trust any single witness. Our proposed scheme allows witnesses to be replaced without jeopardizing the consensus and security in the network. Details on how to change witnesses will be elaborated in Section 3. Transactions in the consensus layer is for the sole purpose of achieving consensus in the network, while real transactions happen in the transaction layer. In the transaction layer, each account has its own chain of blocks, which records the transaction history of this account. In addition, each block in the transaction layer is referenced by blocks in the consensus layer.

The consensus in the Canonchain network is achieved via total ordering of all blocks. Each node starts by finding out the "stable" main chain within the consensus layer of its local DAG. The rigorous definition of stable main chain will be described later in Section 3.1. Each node then numbers all blocks included by blocks on the stable main chain as follows. It first defines indices for blocks that lie directly on the stable main chain. The genesis block has index 0, the next block on the stable main chain that is a child of the genesis block has index 1, and so on. By traveling forward along the stable main chain, it assigns indices to blocks that lie on the stable main chain. For any block that does not lie on the stable main chain, its index is assigned by the index of the block on the stable main chain that first references it directly or indirectly. Now each node can determine the order for any two blocks B_1 and B_2 with assigned indices using the following rule $\mathcal{O}$: B_1 precedes B_2 if and only if

a) B_1 has lower index than B_2; or

b) B_1 and B_2 have the same indices, but B_1 is referenced by B_2 directly or indirectly; or

c) B_1 and B_2 have the same indices, and there is no reference relationship between B_1 and B_2, but B_1 has lower hash than B_2.

As a concrete example shown in Fig. 1, a node is trying to decide the order of two blocks B_1 and B_2 marked in blue. The stable main chain it finds out is marked in bold arrows. And the numbers inside each block are indices assigned according to the stable main chain. Now block B_1 has index 3 and block B_2 has index 4. Therefore, the node will determine that B_1 precedes B_2 since B_1 has lower index than B_2.

3 Consensus in Canonchain

In this section, we will focus on the consensus layer of our R-DAG structure, and explain in detail how a node finds out the stable main chain of its local graph. The remainder of this section is organized as follows. The key terms which will be used intensively throughout the paper are described in Section 3.1. In Section 3.2, we list the key assumptions we rely on in order to guarantee that the Canonchain network is secure. Based on the definitions and assumptions, Section 3.3 presents the consensus algorithm which is implemented in the Canonchain main-net.

3.1 Definitions

At any time, each node in the network would observe slightly different graph due to network delay. Let $\mathsf{G}_n(t)$ denote the graph node n has observed at time t. In this section, we drop n and t and use G to represent a general DAG which satisfies that if a block B is in G, all B's parents are also in G. In the following, we describe some key terms which will be used intensively in the subsequent sections.

D1 Graph inclusion relation: We use $\mathsf{G} \subseteq \mathsf{G}^*$ to represent that G^* contains all blocks in G, and G^* satisfies the condition that if a block B is in G^*, all B's parents are also in G^*.

D2 Block inclusion relation: We say a block B_1 includes another block B_0 if $B_1 = B_0$ or B_1 references B_0 directly or indirectly.

D3 Block comparison: Suppose each block in G has its epoch, level and hash, where the definitions of epoch and level will be discussed in D6 and D7, respectively. For any pair of blocks B_0 and B_1, we call B_1 is better than B_0 if and only if B_1 has larger epoch, or larger level if B_0 and B_1 have the same epoch, or larger hash in the case that B_0 and B_1 have the same epoch and the same level. We denote this comparison rule as $\mathcal{R}$.

D4 Best Parent: The best parent of a block is one of its parents, which is the best under block comparison rule $\mathcal{R}$. The best parent of a block B is denoted by $\mathsf{bp}(B)$.

D5 Block height: The height of a block B, denoted by $\mathsf{h}(B)$, refers to the length of the path from B to the genesis block through best parent links. Note that the height of the genesis block is 0.

D6 Epoch: The system moves through a succession of configurations called epochs. In each epoch, there is a different set of witnesses, denoted by $\mathcal{W}_i$. Let N_i denote the number of witnesses in $\mathcal{W}_i$ and $K_i = \left\lfloor \frac{2}{3} N_i \right\rfloor + 1$. We represent the set of all nonnegative integers as a union of disjoint consecutive integer sequences, i.e., $\mathbb{N} \cup \{0\} = \bigcup_{i=1}^{\infty} \mathcal{I}_i$, where $\mathcal{I}_i$ is a consecutive integer sequence ranging from a_i to b_i. Here, all the numbers in $\mathcal{I}_j$ is larger than those in $\mathcal{I}_i$ for any $j > i$, i.e., $a_j > b_i$.

The epoch a block B belongs to is determined by which interval the height of the last stable block (defined later in D10) of B's best parent falls in. Specifically, if the height of the last stable block of $\mathsf{bp}(B)$ is in $\mathcal{W}_i$, the epoch of block B, denoted by $\mathsf{ep}(B)$, is i.

D7 Block level: The level of a block B, denoted by $\mathsf{lv}(B)$, is defined as follows:

$$\mathsf{lv}(B) = \begin{cases} 0, & \text{if } B \text{ is the genesis block,} \\ 1, & \text{if } \mathsf{ep}(B) > \mathsf{ep}\big(\mathsf{bp}(B)\big), \\ \mathsf{lv}\big(\mathsf{bp}(B)\big) + 1, & \text{if } \mathsf{ep}(B) = \mathsf{ep}\big(\mathsf{bp}(B)\big). \end{cases} \tag{1}$$

D8 Main chain: The main chain of graph G is defined as the path starting from the best tip block in G under block comparison rule $\mathcal{R}$ to the genesis block through best parent links. Here, tip blocks refer to blocks without any child.

D9 Stable block: A block on the main chain of G is called a stable block of G if it is guaranteed to be contained in the main chain of any graph G^* that includes G, i.e., $\mathsf{G} \subseteq \mathsf{G}^*$.

D10 Last stable block: The last stable block of the genesis block is itself. Now for a block B_1, given that the last stable block of its best parent is defined, the last stable block of B_1 is determined by the following procedure. For any two blocks B and B^*, we use $B^* \rightarrow B$ to denote that B^* includes B through parent links and all blocks in the path (including both B^* and B) must be in the same epoch. Similarly, we use $B^* \xrightarrow{b} B$ to denote that B^* includes B through best parent links and all blocks in the path need not be in the same epoch. The degenerated case of $B = B^*$ is regarded true, i.e., $B^* \rightarrow B$ and $B^* \xrightarrow{b} B$. For any block B_0 such that $B_1 \xrightarrow{b} B_0$, let $\mathsf{C}(B_0, B_1)$ denote the set of blocks from B_1 to B_0 through best parent links, which includes B_1 but not B_0. Assume $\mathsf{ep}(B_1) = i$. Start with $B_0 = \mathsf{lsb}\big(\mathsf{bp}(B_1)\big)$, and check whether the following condition holds

$$\mathsf{lv}(B_1) > \max_{B \in \mathsf{S}(B_0, B_1)} \mathsf{lv}(B) + 2(K_i - 1), \tag{2}$$

where $\mathsf{S}(B_0, B_1) = \Big\{ B \Big| B \xrightarrow{b} B_0, B_1 \rightarrow B, \mathsf{C}(B_0, B) \bigcap \mathsf{C}(B_0, B_1) = \emptyset \Big\}$. If $\mathsf{S}(B_0, B_1) = \emptyset$, the maximal value over $\mathsf{S}(B_0, B_1)$ in (2) is set to be 0. If the condition (2) holds, update B_0 to be its child on $\mathsf{C}(B_0, B_1)$

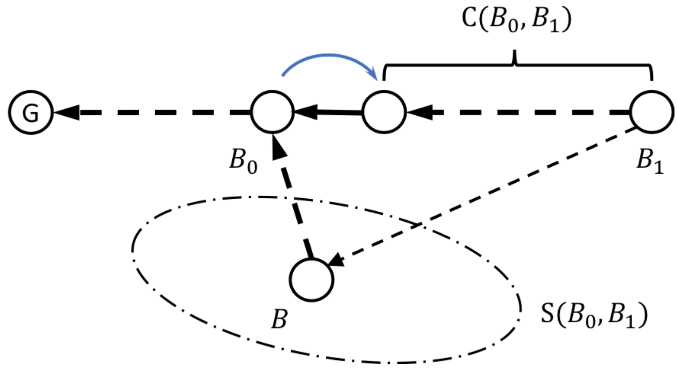

Figure 2: One step in finding out the last stable block of B_1. Solid and dashed lines represent parent-child links and ancestor-descendant links, respectively. Bold and regular lines represent $\xrightarrow{b}$ and $\rightarrow$ relations, respectively.

and go back to check the condition (2) again, and so on. We repeatedly advance B_0 till $\mathsf{h}(B_0) \in \mathcal{I}_{i+1}$ or B_1 does not satisfy the condition (2) with respect to B_0. The block B_0 we stop at is the last stable block of B_1, denoted by $\mathsf{lsb}(B_1)$. One advancement of B_0 described above is depicted as the blue arrow in Fig. 2.

D11 Stable main chain: From the last stable blocks of all blocks in G, we pick the one with the largest height, denoted by $\mathsf{SB}(\mathsf{G})$. The stable main chain of G, denoted by $\mathsf{SC}(\mathsf{G})$, is then defined as the chain of blocks starting from $\mathsf{SB}(\mathsf{G})$ to the genesis block through best parent links. Note that the stable main chain of G is part of the main chain that will not change as G expands.

D12 Main chain index (MCI): The MCI for any block that lies directly on the stable main chain is equal to its height. For any block that does not lie on the main chain, its MCI is assigned by the MCI of the block on the stable main chain that first includes it. The MCI of a block B is denoted by $\mathsf{mci}(B)$.

Many definitions above depend on each other. However, they can be incrementally built up as the DAG grows. To start with, the genesis block belongs to epoch 0, has level 0 and its last stable block is itself. For a new block B added to the graph, assume that all terms for its parents are already well defined. We first find out its best parent $\mathsf{bp}(B)$ via block comparison rule $\mathcal{R}$. Next, we find out its epoch $\mathsf{ep}(B)$ by checking the height of the last stable block of $\mathsf{bp}(B)$. B's level $\mathsf{lv}(B)$ can then be determined by (1). And the last step is to find out the last stable block of B, i.e., $\mathsf{lsb}(B)$ by the procedure described in D10. After that, we will know whether the stable main chain of the graph has been extended or not.

3.2 Assumptions

The key assumptions used in Canonchain consensus protocol and subsequent technical discussions are as follows:

A1 Honest witnesses should generate blocks serially. In other words, each honest witness should reference (directly or indirectly) all its previous blocks in every subsequent block.

A2 When an honest witness composes a block, he always chooses the best tip block of its local graph under block comparison rule $\mathcal{R}$ as the best parent of this new block.

A3 If a block is in epoch i, the issuer of this block must be in the witness set $\mathcal{W}_i$.

A4 Start from any block in epoch i and traverse through best parent links, we stop as soon as we encounter K_i blocks or a block of level 1, whichever comes first. Each block we encountered (including the one we stop at) must be issued by a different witness from the witness set $\mathcal{W}_i$.

A5 In each epoch i, more than 2/3 of the witnesses in $\mathcal{W}_i$ are honest. In other words, at least K_i witnesses are honest, where $K_i = \left\lfloor \frac{2}{3} N_i \right\rfloor + 1$ is defined in D6.

A6 Any block will be delivered to all honest witnesses within some fixed but unknown amount of time. It implies that for honest witnesses, the graphs they eventually observe would be consistent with each other. That is to say, for any pair of honest witnesses i and j, the graph $\mathsf{G}_i(t_i)$ node i observed at time t_i will also be observed by node j at some time t_j, i.e., $\mathsf{G}_i(t_i) \subseteq \mathsf{G}_j(t_j)$.

The assumptions from A1 to A4 are also constraints that need to be satisfied when a witness issues a block. Among those, however, only A3 and A4 are binding. That is to say, other witnesses can perform certain sanity check on A3 and A4, and reject the block if either of these two conditions is not met. Note that assumption A6 is a form of partial asynchrony [9], which is a middle ground between synchrony and asynchrony.

Algorithm 1 Canonchain Consensus Algorithm

Input: Local graph $\mathsf{G} = \{G\}$ for some node, where G is the genesis block
Initialization: Set $\mathsf{ep}(G) = 0, \mathsf{lv}(G) = 0, \mathsf{lsb}(G) = G$.
Main iterations:
for all received block B_1 **do**
  if B_1 does not pass the sanity checks **then**
    Reject block B_1.
    Continue
  end if
  if At least one of B_1's parent is not in G **then**
    Add block B_1 into a buffer for future consideration.
    Continue
  end if
  if B_1 is not issued by a witness **then**
    Continue
  end if
  Determine B_1's best parent $\mathsf{bp}(B_1)$ by block comparison rule $\mathcal{R}$.
  Determine B_1's epoch $\mathsf{ep}(B_1)$ by checking which interval the height of $\mathsf{lsb}\big(\mathsf{bp}(B_1)\big)$ falls in. Assume the interval is $\mathcal{I}_i$, i.e., $\mathsf{ep}(B_1) = i$.
  if Assumptions A3 or A4 is not satisfied **then**
    Reject block B_1.
    Continue
  end if
  Add B_1 to G, and determine B_1's level $\mathsf{lv}(B_1)$ according to (1).
  Set $B_0 = \mathsf{lsb}\big(\mathsf{bp}(B_1)\big)$.
  while The condition (2) holds **do**
    Update B_0 to be its child in $\mathsf{C}(B_0, B_1)$.
  end while
  Set $\mathsf{lsb}(B_1) = B_0$.
  if $\mathsf{lsb}(B_1)$ has larger height than the tip block of the existing stable main chain **then**
    Update the stable main chain $\mathsf{SC}(\mathsf{G})$ to end with $\mathsf{SB}(\mathsf{G}) = \mathsf{lsb}(B_1)$.
  end if
  Find out MCIs of all blocks that are included by any block on $\mathsf{SC}(\mathsf{G})$.
end for
Output: Linear ordering of all blocks that are included by any block on $\mathsf{SC}(\mathsf{G})$ using rule $\mathcal{O}$.

3.3 Consensus Algorithm

Based on the definitions and assumptions above, the consensus algorithm implemented in Canonchain is summarized in Algorithm 1. The key idea is on how to consistently expand the local graph when receiving a block. For consensus purpose, we only need to deal with blocks issued by witnesses and update the stable main chain accordingly, since only those blocks can contribute to the consensus of the system.

4 Correctness

This section provides the technical proofs to show that the consensus algorithm described in Algorithm 1 is correct. Section 4.1 provides some useful propositions that will be used in the subsequent sections. In Section 4.2, we show that the advance of last stable block defined in D10 guarantees that the last stable block is indeed stable. Section 4.3 and Section 4.4 are dedicated to prove that our consensus algorithm satisfies safety and liveness properties, respectively. Note that in this section, we still focus on the consensus layer of our R-DAG structure.

4.1 Propositions

Recall that for any two blocks B and B^*, $B^* \to B$ denotes that B^* includes B through parent links and all blocks in the path (including both B^* and B) are in the same epoch. Similarly, $B^* \xrightarrow{b} B$ denotes that B^* inlcudes B through best parent links and all blocks in the path are not necessarily in the same epoch. In the following, we prove some useful results which will be used in later analysis.

Proposition 1. *For any two blocks B_0 and B_1, if $B_0 = \mathsf{bp}(B_1)$, we have $\mathsf{lsb}(B_1) \xrightarrow{b} \mathsf{lsb}(B_0)$, and $\mathsf{ep}(B_1) = \mathsf{ep}(B_0)$ or $\mathsf{ep}(B_1) = \mathsf{ep}(B_0) + 1$.*

Proof. It can be directly inferred from how the last stable block is determined as described in D10. To find the last stable block of B_1, we start with $B^* = \mathsf{lsb}(B_0)$, and update B^* to be its child in $\mathsf{C}(B^*, B_1)$ in each step as long as B_1 satisfies the condition (2) with respect to B^*. It guarantees that in every step, the new B^* references the old one through the best parent link. Therefore, we have $\mathsf{lsb}(B_1) \xrightarrow{b} \mathsf{lsb}(B_0)$. Assume $\mathsf{ep}(B_0) = i$, i.e., $\mathsf{h}\big(\mathsf{lsb}\big(\mathsf{bp}(B_0)\big)\big) \in \mathcal{I}_i$. To find the last stable block of B_0, the block we stop at, i.e., $\mathsf{lsb}(B_0)$ must satisfy that $\mathsf{h}\big(\mathsf{lsb}(B_0)\big)$ is still in $\mathcal{I}_i$ or in $\mathcal{I}_{i+1}$.

It follows that $\mathsf{ep}(B_1) = i$ or $i+1$, which leads to $\mathsf{ep}(B_1) = \mathsf{ep}(B_0)$ or $\mathsf{ep}(B_1) = \mathsf{ep}(B_0) + 1$. $\square$

Proposition 2. *For any two blocks B_0 and B_1, if B_1 includes B_0, we have $\mathsf{ep}(B_1) \geq \mathsf{ep}(B_0)$.*

Proof. The statement is true for the trivial case $B_0 = B_1$. Now we assume that $B_0 \neq B_1$. First, we show that if B_0 is a parent of B_1, $\mathsf{ep}(B_1) \geq \mathsf{ep}(B_0)$ holds. Consider the following two cases.

1) B_0 is the best parent of B_1: We have $\mathsf{lsb}(B_0) \xrightarrow{b} \mathsf{lsb}\big(\mathsf{bp}(B_0)\big)$ by Proposition 1. It follows that $\mathsf{h}\big(\mathsf{lsb}(B_0)\big) \geq \mathsf{h}\big(\mathsf{lsb}\big(\mathsf{bp}(B_0)\big)\big)$. Thus, there exists $i \geq j$ such that $\mathsf{h}\big(\mathsf{lsb}(B_0)\big) \in \mathcal{I}_i$ and $\mathsf{h}\big(\mathsf{lsb}\big(\mathsf{bp}(B_0)\big)\big) \in \mathcal{I}_j$. Therefore, $\mathsf{ep}(B_1) = i \geq j = \mathsf{ep}(B_0)$.

2) $B_2 \neq B_0$ is the best parent of B_1: Similarly as in the previous case, we have $\mathsf{ep}(B_1) \geq \mathsf{ep}(B_2)$. According to the definition of best parent, B_2 is better than B_0 under block comparison rule $\mathcal{R}$. It implies that $\mathsf{ep}(B_2) \geq \mathsf{ep}(B_0)$. Therefore, we have $\mathsf{ep}(B_1) \geq \mathsf{ep}(B_2) \geq \mathsf{ep}(B_0)$.

For the general case that B_1 does not directly reference B_0, we can apply the chain rule to show that $\mathsf{ep}(B_1) \geq \mathsf{ep}(B_0)$. $\square$

Proposition 3. *For any two blocks B_0 and B_1, if $B_1 \to B_0$, we have $\mathsf{lv}(B_1) \geq \mathsf{lv}(B_0)$.*

Proof. The statement is true for the trivial case $B_0 = B_1$. Now we assume that $B_0 \neq B_1$. First, we show that if B_0 is a parent of B_1, $\mathsf{lv}(B_1) \geq \mathsf{lv}(B_0)$ holds. Consider the following two cases.

1) B_0 is the best parent of B_1: Since B_0 and B_1 are in the same epoch by the definition of $B_1 \to B_0$, we have $\mathsf{lv}(B_1) = \mathsf{lv}(B_0) + 1 > \mathsf{lv}(B_0)$ by (1).

2) $B_2 \neq B_0$ is the best parent of B_1: According to the definition of best parent, B_2 is better than B_0 under block comparison rule $\mathcal{R}$. It implies that $\mathsf{ep}(B_2) \geq \mathsf{ep}(B_0)$. It follows that

$$\mathsf{ep}(B_2) \geq \mathsf{ep}(B_0) \overset{(a)}{=} \mathsf{ep}(B_1) \overset{(b)}{\geq} \mathsf{ep}(B_2), \tag{3}$$

where (a) is by the definition of $B_1 \to B_0$ and (b) is by Proposition 2. Thus, the following condition holds: $\mathsf{ep}(B_0) = \mathsf{ep}(B_1) = \mathsf{ep}(B_2)$. Therefore, we have

$$\mathsf{lv}(B_1) \overset{(a)}{=} \mathsf{lv}(B_2) + 1 \overset{(b)}{\geq} \mathsf{lv}(B_0) + 1 > \mathsf{lv}(B_0), \tag{4}$$

where (a) is by (1) and (b) is due to the fact that $\mathsf{lv}(B_2) \geq \mathsf{lv}(B_0)$ since B_2 is better than B_0 under $\mathcal{R}$ but $\mathsf{ep}(B_0) = \mathsf{ep}(B_2)$.

For the general case that B_1 does not directly reference B_0, we can apply the chain rule to show that $\mathsf{lv}(B_1) \geq \mathsf{lv}(B_0)$. $\square$

The following is a direct corollary of Proposition 2 and Proposition 3.

Corollary 1. *For any two blocks B_0 and B_1, if B_1 includes B_0 and $\mathsf{ep}(B_1) = \mathsf{ep}(B_0)$, we have $B_1 \to B_0$ and $\mathsf{lv}(B_1) \geq \mathsf{lv}(B_0)$.*

4.2 Advance of Last Stable Block

Let G^B denote the induced graph from a block B in G which consists of all blocks that B includes. In this section, we will analyze the procedure to determine the last stable block of B, i.e., $\mathsf{lsb}(B)$. Our main goal is to show that $\mathsf{lsb}(B)$ is a stable block of graph G^B. Recall that from Assumption A4, if we start from block B in epoch i, traverse through best parents links, and stop as soon as K_i blocks or a block of level 1 has been visited, all blocks encountered must be issued by different witnesses from the witness set $\mathcal{W}_i$. Let $\mathsf{T}(B)$ and $\mathsf{W}(B)$ denote the set of blocks encountered and the set of witnesses who issue these blocks, respectively. Note that all blocks in set $\mathsf{T}(B)$ are in the same epoch as B. In the following, we first prove three lemmas which are crucial for the proof of our claim.

Lemma 1. *If $B_1 \xrightarrow{b} B_0$, all blocks in $\mathsf{C}(B_0, B_1)$ are in epoch i and none of them is issued by an honest witness from a set $\mathcal{W} \subseteq \mathcal{W}_i$ which consists of K_i witnesses, then $\mathsf{C}(B_0, B_1)$ contains at most $K_i - 1$ blocks, i.e., $|\mathsf{C}(B_0, B_1)| \leq K_i - 1$.*

Proof. Since all blocks in $\mathsf{C}(B_0, B_1)$ are issued by witnesses from set $\mathcal{W}_i$ and none of them is issued by an honest witness from $\mathcal{W}$, they can only be issued by $N_i - K_i$ witnesses outside $\mathcal{W}$ and malicious witnesses inside $\mathcal{W}$, which is at most $N_i - K_i$ by Assumption A5. Thus, due to $K_i > \frac{2}{3}N_i$ in assumption A5, the number of distinct witnesses which have issued at least one block in $\mathsf{C}(B_0, B_1)$ is at most

$$2(N_i - K_i) < \frac{2}{3}N_i < K_i \,. \tag{5}$$

It then follows from Assumption A4 that $|\mathsf{C}(B_0, B_1)| < K_i$, which is equivalent to $|\mathsf{C}(B_0, B_1)| \leq K_i - 1$. It completes the proof of Lemma 1. $\square$

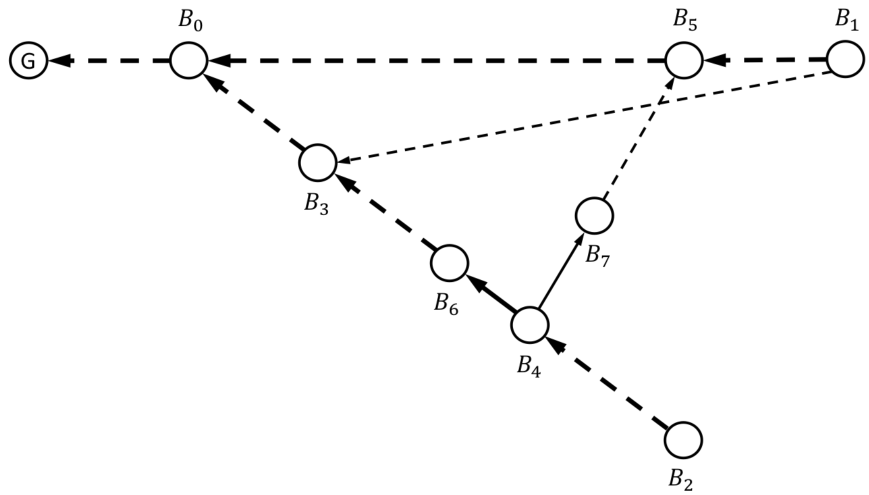

Figure 3: The case $\mathsf{ep}(B_0) = i$. Solid and dashed lines represent parent-child links and ancestor-descendant links, respectively. Bold and regular lines represent $\xrightarrow{b}$ and $\rightarrow$ relations, respectively.

Lemma 2. *If $B_1 \xrightarrow{b} B_0$, $\mathsf{ep}(B_1) = i$ and B_1 satisfies the condition* (2) *with respect to B_0, for any block B_2 such that $\mathsf{ep}(B_2) = i$, $B_2 \xrightarrow{b} B_0$ and $\mathsf{C}(B_0, B_2) \bigcap \mathsf{C}(B_0, B_1) = \emptyset$, we have $\mathsf{lv}(B_2) < \mathsf{lv}(B_1)$.*

Proof. Since $\mathsf{ep}(B_0) \leq \mathsf{eq}(B_1) = i$ by Proposition 2, in the following we consider two cases, namely $\mathsf{ep}(B_0) = i$ or $\mathsf{ep}(B_0) < i$.

First, consider the case $\mathsf{ep}(B_0) = i$. It means that $\mathsf{S}(B_0, B_1) \neq \emptyset$ since $B_0 \in \mathsf{S}(B_0, B_1)$. We start from B_2, traverse through best parent links till B_0, and stop as soon as a block in $\mathsf{S}(B_0, B_1)$ is encountered. Let B_3 denote the block we stop at, i.e.,

$$B_3 = \underset{B \in (\mathsf{C}(B_0,B_2) \bigcup \{B_0\}) \bigcap \mathsf{S}(B_0,B_1)}{\arg\max} \mathsf{lv}(B). \tag{6}$$

We show that no block in $\mathsf{C}(B_3, B_2)$ is issued by any honest witness from set $\mathsf{W}(B_1)$. It is proved by contradiction. Assume there are blocks in $\mathsf{C}(B_3, B_2)$ issued by honest witnesses from $\mathsf{W}(B_1)$. Among those, let B_4 denote the one with the smallest height. As shown in Fig. 3, let B_5 denote the block in set $\mathsf{T}(B_1)$ which comes from the same witness as B_4. Since B_4 and B_5 come from the same honest witness, by Assumption A1, either B_4 includes B_5 or B_5 includes B_4. Since B_2 includes B_3 and $\mathsf{ep}(B_2) = \mathsf{ep}(B_3) = i$, we have $\mathsf{ep}(B_4) = i$ by Corollary 1. Similarly, we have $\mathsf{ep}(B_5) = \mathsf{ep}(B_1) = i$.

Therefore, by Corollary 1, either $B_4 \to B_5$ or $B_5 \to B_4$ holds. However, by the definition of B_3 in (6), which is the first block included by B_1 when traversing from B_2 through best parent links, it is impossible that $B_5 \to B_4$. Thus, we have $B_4 \to B_5$. Let B_6 and B_7 be parents of B_4 such that $B_4 \xrightarrow{b} B_6$ and $B_7 \to B_5$, respectively. Since $\mathsf{ep}(B_2) = \mathsf{ep}(B_3) = i$, all blocks in $\mathsf{C}(B_3, B_6)$ are in epoch i by Corollary 1. By the definition of B_4, no block in $\mathsf{C}(B_3, B_6)$ is issued by any honest witness from $\mathsf{W}(B_1)$. In addition, the cardinality of $\mathsf{W}(B_1)$ is K_i since B_1 satisfies the condition (2), which implies that $\mathsf{lv}(B_1) > K_i$. Therefore, by Lemma 1, we have $|\mathsf{C}(B_3, B_6)| \leq K_i - 1$, which leads to

$$\mathsf{lv}(B_6) \leq \mathsf{lv}(B_3) + (K_i - 1)\,. \tag{7}$$

Now the following chain of inequalities hold

$$\mathsf{lv}(B_7) \overset{(a)}{\geq} \mathsf{lv}(B_5) \overset{(b)}{\geq} \mathsf{lv}(B_1) - (K_i - 1) \overset{(c)}{>} \mathsf{lv}(B_3) + (K_i - 1) \overset{(d)}{\geq} \mathsf{lv}(B_6), \tag{8}$$

where (a) is by Proposition 3, (b) is due to $B_5 \in \mathsf{T}(B_1)$, (c) is by the fact that $B_3 \in \mathsf{S}(B_0, B_1)$ and B_1 satisfies the condition (2) with respect to B_0, and (d) is by (7). It contradicts with the fact that $\mathsf{lv}(B_6) \geq \mathsf{lv}(B_7)$ since B_6 is the best parent of B_4 and $\mathsf{ep}(B_6) = \mathsf{ep}(B_7) = i$. It completes the proof that no block in $\mathsf{C}(B_3, B_2)$ is issued by any honest witness from $\mathsf{W}(B_1)$. In addition, $B_2 \xrightarrow{b} B_3$ and all blocks in $\mathsf{C}(B_3, B_2)$ are in epoch i, by Lemma 1 we have $|\mathsf{C}(B_3, B_2)| \leq K_i - 1$, which leads to

$$\mathsf{lv}(B_2) \leq \mathsf{lv}(B_3) + (K_i - 1)\,. \tag{9}$$

It follows that

$$\mathsf{lv}(B_1) \overset{(a)}{>} \mathsf{lv}(B_3) + 2(K_i - 1) \overset{(b)}{\geq} \mathsf{lv}(B_2) + (K_i - 1) \geq \mathsf{lv}(B_2), \tag{10}$$

where (a) is by the fact that $B_3 \in \mathsf{S}(B_0, B_1)$ and B_1 satisfies the condition (2) with respect to B_0, and (b) is by (9). It competes the proof that $\mathsf{lv}(B_2) < \mathsf{lv}(B_1)$ if $\mathsf{ep}(B_0) = i$.

Next, we consider the case $\mathsf{ep}(B_0) < i$. If $\mathsf{S}(B_0, B_1) \neq \emptyset$, we can follow the same arguments as in the previous proof to show that $\mathsf{lv}(B_2) < \mathsf{lv}(B_1)$. Now we assume $\mathsf{S}(B_0, B_1) = \emptyset$. Since $\mathsf{ep}(B_2) = i > \mathsf{ep}(B_0)$, by Proposition 1, there exits a block $B_3 \in \mathsf{C}(B_0, B_2)$ such that $\mathsf{ep}(B_3) = i$ and $\mathsf{ep}\big(\mathsf{bp}(B_3)\big) = i - 1$, i.e., $\mathsf{lv}(B_3) = 1$. Similarly as in the previous case, we show that no block in $\mathsf{C}\big(\mathsf{bp}(B_3), B_2\big)$ is issued by any honest witness from set $\mathsf{W}(B_1)$. It is also proved by contradiction. Assume there are blocks in $\mathsf{C}\big(\mathsf{bp}(B_3), B_2\big)$ issued by honest witnesses from $\mathsf{W}(B_1)$. Among those, let B_4

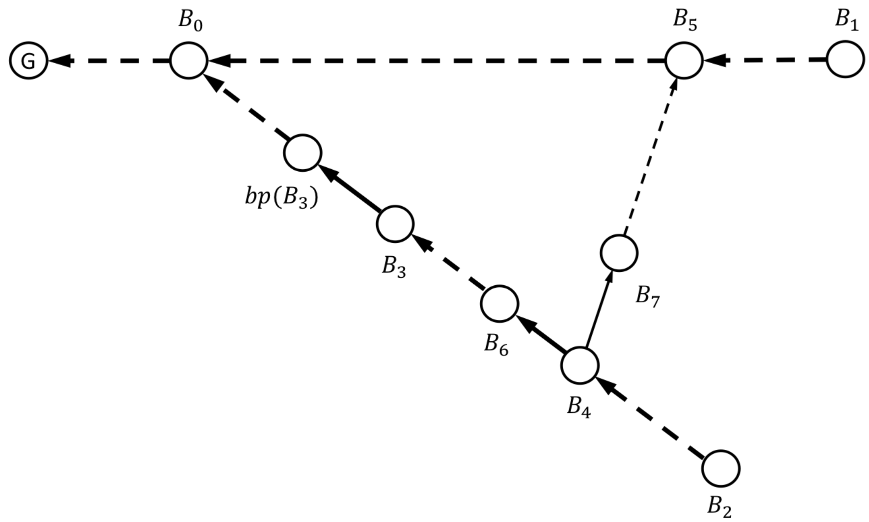

Figure 4: The case $\mathsf{ep}(B_0) < i$. Solid and dashed lines represent parent-child links and ancestor-descendant links, respectively. Bold and regular lines represent $\xrightarrow{b}$ and $\rightarrow$ relations, respectively.

denote the one with the smallest height. As shown in Fig. 4, let B_5 denote the block in set $\mathsf{T}(B_1)$ which comes from the same witness as B_4 . Since B_4 and B_5 come from the same honest witness, by Assumption A1, either B_4 includes B_5 or B_5 includes B_4. Since B_2 includes B_3 and $\mathsf{ep}(B_2) = \mathsf{ep}(B_3)$, we have $\mathsf{ep}(B_4) = i$ by Corollary 1. Also we have $\mathsf{ep}(B_5) = \mathsf{ep}(B_1) = i$. Therefore, by Corollary 1, either $B_4 \rightarrow B_5$ or $B_5 \rightarrow B_4$ holds. However, it is impossible that $B_5 \rightarrow B_4$ since it is assumed that $\mathsf{S}(B_0, B_1) = \emptyset$. Thus, we have $B_4 \rightarrow B_5$. Let B_6 and B_7 be parents of B_4 such that $B_4 \xrightarrow{b} B_6$ and $B_7 \rightarrow B_5$, respectively. If $B_4 = B_3$, we have

$$\mathsf{ep}(B_6) = \mathsf{ep}\big(\mathsf{bp}(B_3)\big) = i - 1 < i = \mathsf{ep}(B_5) \leq \mathsf{ep}(B_7), \tag{11}$$

where the last inequality is due to Proposition 2. It contradicts with the fact that B_6 is the best parent of B_4. If $B_4 \neq B_3$, by the definition of B_4, no block in $\mathsf{C}\big(\mathsf{bp}(B_3), B_6\big)$ is issued by any honest witness from $\mathsf{W}(B_1)$. And all blocks in $\mathsf{C}\big(\mathsf{bp}(B_3), B_6\big)$ are in epoch i. Therefore, by Lemma 1, we have $|\mathsf{C}\big(\mathsf{bp}(B_3), B_6\big)| \leq K_i - 1$, which leads to

$$\mathsf{lv}(B_6) \leq K_i - 1\,, \tag{12}$$

since $\mathsf{lv}(B_3) = 1$. In the following, we derive a similar chain of inequalities as (8):

$$\mathsf{lv}(B_7) \overset{(a)}{\geq} \mathsf{lv}(B_5) \overset{(b)}{\geq} \mathsf{lv}(B_1) - (K_i - 1) \overset{(c)}{>} K_i - 1 \overset{(d)}{\geq} \mathsf{lv}(B_6), \tag{13}$$

where (a) is by Proposition 3, (b) is due to $B_5 \in \mathsf{T}(B_1)$, (c) is by the fact that B_1 satisfies the condition (2) which implies $\mathsf{lv}(B_1) > 2(K_i - 1)$, and (d) is from (12). It contradicts with the fact that $\mathsf{lv}(B_6) \geq \mathsf{lv}(B_7)$ since B_6 is the best parent of B_4 and $\mathsf{ep}(B_6) = \mathsf{ep}(B_7) = i$. It completes the proof that no block in $\mathsf{C}\big(\mathsf{bp}(B_3), B_2\big)$ is issued by any honest witness from $\mathsf{W}(B_1)$. In addition, $B_2 \xrightarrow{b} \mathsf{bp}(B_3)$ and all blocks in $\mathsf{C}\big(\mathsf{bp}(B_3), B_2\big)$ are in epoch i, by Lemma 1 we have $|\mathsf{C}\big(\mathsf{bp}(B_3), B_2\big)| \leq K_i - 1$, which leads to

$$\mathsf{lv}(B_2) \leq K_i - 1\,, \tag{14}$$

since $\mathsf{lv}(B_3) = 1$. It follows that

$$\mathsf{lv}(B_1) \overset{(a)}{>} 2(K_i - 1) \overset{(b)}{\geq} \mathsf{lv}(B_2) + (K_i - 1) \geq \mathsf{lv}(B_2), \tag{15}$$

where (a) is by the fact that B_1 satisfies the condition (2) which implies $\mathsf{lv}(B_1) > 2(K_i - 1)$, and (b) is by (14). It competes the proof that $\mathsf{lv}(B_2) < \mathsf{lv}(B_1)$ if $\mathsf{ep}(B_0) < i$.

By combining the two cases above, we finish the proof of Lemma 2. □

Lemma 3. *Given $i \in \mathbb{N}$, assume $\mathsf{lsb}(B)$ is a stable block of graph G^B for any block B with $\mathsf{ep}(B) < i$. If $B_1 \xrightarrow{b} B_0$, $\mathsf{ep}(B_1) = i$, $\mathsf{h}(B_0) \in \mathcal{I}_i$ and B_1 satisfies the condition (2) with respect to B_0, for any block B_2 such that $B_2 \xrightarrow{b} B_0$ and $\mathsf{C}(B_0, B_2) \bigcap \mathsf{C}(B_0, B_1) = \emptyset$, we have $\mathsf{ep}(B_2) \leq \mathsf{ep}(B_1)$.*

Proof. According to the procedure of determining the last stable block in D10, we have $B_2 \xrightarrow{b} \mathsf{lsb}(B_2)$. Since $B_2 \xrightarrow{b} B_0$, either $B_0 \xrightarrow{b} \mathsf{lsb}(B_2)$ or $\mathsf{lsb}(B_2) \xrightarrow{b} B_0$ holds. We show that $B_0 \xrightarrow{b} \mathsf{lsb}(B_2)$. It is proved by contradiction. Suppose $\mathsf{lsb}(B_2) \xrightarrow{b} B_0$ and $\mathsf{lsb}(B_2) \neq B_0$, which means that the last stable block of B_2 has advanced past B_0. Thus, there exists some block $B_3 \in \mathsf{C}(B_0, B_2)$ such that B_3 satisfies the condition (2) with respect to B_0, i.e.,

$$\mathsf{lv}(B_3) > \max_{B \in \mathsf{S}(B_0, B_3)} \mathsf{lv}(B) + 2(K_j - 1), \tag{16}$$

where $j = \mathsf{ep}(B_3) \leq \mathsf{ep}(B_2) = i$ by Proposition 2. And the last stable block of B_3 has advanced past B_0, i.e., $\mathsf{lsb}(B_3) \in \mathsf{C}(B_0, B_2)$. Consider the following two cases.

1) $j < i$: Let $\mathsf{G}^* = \mathsf{G}^{B_3} \bigcup \mathsf{G}^{B_1}$. Since $\mathsf{ep}(B_3) < \mathsf{ep}(B_1)$, B_1 is the tip block of the main chain of G^*. By the assumption in the statement of Lemma 3, $\mathsf{lsb}(B_3)$ is a stable block of graph G^{B_3}. Due to $\mathsf{G}^{B_3} \subseteq \mathsf{G}^*$, $\mathsf{lsb}(B_3)$ is on the main chain of G^*, i.e., $B_1 \xrightarrow{b} \mathsf{lsb}(B_3)$. It contradicts with the fact that $\mathsf{lsb}(B_3) \in \mathsf{C}(B_0, B_2)$ and $\mathsf{C}(B_0, B_2) \bigcap \mathsf{C}(B_0, B_1) = \emptyset$.

2) $j = i$: Since both B_1 and B_3 satisfy the condition (2) with respect to B_0, it follows by Lemma 2 that both $\mathsf{lv}(B_3) < \mathsf{lv}(B_1)$ and $\mathsf{lv}(B_1) < \mathsf{lv}(B_3)$ hold, which is a contradiction.

Now we have shown that $B_0 \xrightarrow{b} \mathsf{lsb}(B_2)$. In addition, we have $\mathsf{lsb}(B_2) \xrightarrow{b} \mathsf{lsb}\big(\mathsf{bp}(B_2)\big)$ by Proposition 1. Thus, $B_0 \xrightarrow{b} \mathsf{lsb}\big(\mathsf{bp}(B_2)\big)$ holds. It follows that $\mathsf{h}\Big(\mathsf{lsb}\big(\mathsf{bp}(B_2)\big)\Big) \le \mathsf{h}(B_0)$. Since $\mathsf{h}(B_0) \in \mathcal{I}_i$, there exists $k \le i$ such that $\mathsf{h}\Big(\mathsf{lsb}\big(\mathsf{bp}(B_2)\big)\Big) \in \mathcal{I}_k$, which leads to $\mathsf{ep}(B_2) = k \le i = \mathsf{ep}(B_1)$. It completes the proof of Lemma 3. □

Now we can prove the following main result of this section.

Theorem 1. *For any block B_1 in graph G, the last stable block of B_1, i.e., $\mathsf{lsb}(B_1)$ is a stable block of graph G^{B_1}.*

Proof. We prove by induction. It is trivial for the case that B_1 is the genesis block. For the case $\mathsf{ep}(B_1) = i$, we assume that for any block B such that $\mathsf{ep}(B) < i$ or $B = \mathsf{bp}(B_1)$, $\mathsf{lsb}(B)$ is a stable block of G^B. We will prove that $\mathsf{lsb}(B_1)$ is a stable block of graph G^{B_1}.

We first show that for any block B_0 such that B_0 is a stable block of G^{B_1}, $\mathsf{h}(B_0) \in \mathcal{I}_i$, and B_1 satisfies the condition (2) with respect to B_0, then B_0's child in $\mathsf{C}(B_0, B_1)$, denoted by B_0^*, is also a stable block of G^{B_1}. It is equivalent to show that B_0^* is on the main chain of any graph G^* such that $\mathsf{G}^{B_1} \subseteq \mathsf{G}^*$. We prove by contradiction. Assume there exists a graph G^* such that $\mathsf{G}^{B_1} \subseteq \mathsf{G}^*$ and the main chain of G^* does not contain B_0^*. As depicted in Fig. 5, let B_2 denote the tip block of the main chain of G^*. Since B_0 is a stable block of G^{B_1} and $\mathsf{G}^{B_1} \subseteq \mathsf{G}^*$, the main chain of G^* must contain B_0, i.e., $B_2 \xrightarrow{b} B_0$. Now we have $\mathsf{C}(B_0, B_2) \bigcap \mathsf{C}(B_0, B_1) = \emptyset$. It follows that $\mathsf{ep}(B_2) \le \mathsf{ep}(B_1)$ by Lemma 3. Furthermore, if $\mathsf{ep}(B_2) = \mathsf{ep}(B_1) = i$, we have $\mathsf{lv}(B_2) < \mathsf{lv}(B_1)$ by Lemma 2. Therefore, either $\mathsf{ep}(B_2) < \mathsf{ep}(B_1)$ or $\mathsf{lv}(B_2) < \mathsf{lv}(B_1)$ when $\mathsf{ep}(B_2) = \mathsf{ep}(B_1)$ holds, which implies that B_1 is better than B_2 under block comparison rule $\mathcal{R}$. It contradicts with the fact that B_2 is the tip block of the main chain of G^* which contains both B_1 and B_2.

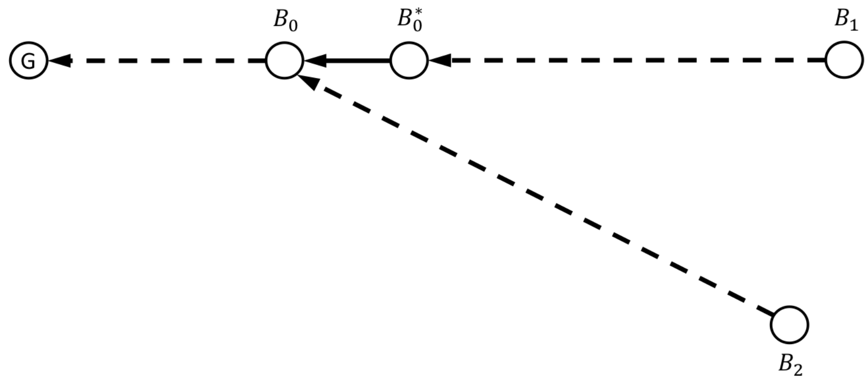

Figure 5: The case where B_0^* is not a stable block of G^{B_1}. Solid and dashed lines represent parent-child links and ancestor-descendant links, respectively.

We start with $B_0 = \mathsf{lsb}\big(\mathsf{bp}(B_1)\big)$. Since $\mathsf{ep}(B_1) = i$, we have $\mathsf{h}(B_0) \in \mathcal{I}_i$. In addition, B_0 is a stable block of $\mathsf{G}^{\mathsf{bp}(B_1)}$ by our assumption. And since $\mathsf{G}^{\mathsf{bp}(B_1)} \subseteq \mathsf{G}^{B_1}$, B_0 is also a stable block of G^{B_1}. Thus, by the result we have proved above, B_0's child in $\mathsf{C}(B_0, B_1)$, denoted by B_0^*, is a stable block of G^{B_1}. We set B_0 to be B_0^*, and repeat this process until $\mathsf{h}(B_0) \notin \mathcal{I}_i$ or B_1 does not satisfy the condition (2) with respect to B_0. The block we stop at, i.e., the last stable block of B_1 is a stable block of G^{B_1}. It completes the proof of Theorem 1. □

4.3 Safety

Recall that the local graph node i observes at time t is denoted by $\mathsf{G}_i(t)$. To determine the order of two blocks at time t, node i will first find the stable main chain of $\mathsf{G}_i(t)$, i.e., $\mathsf{SC}\big(\mathsf{G}_i(t)\big)$, and then find out the order of these two blocks by rule $\mathcal{O}$ in Section 2 given both of them have main chain indices (defined in D12). Therefore, in order to show the safety property of our consensus algorithm, it suffices to prove that the stable main chains different nodes observe at different time are consistent, which is stated in the following Theorem 2.

Theorem 2. *For any $i, j \in \mathbb{N}$ and $t_i, t_j \geq 0$, we have either $\mathsf{SC}\big(\mathsf{G}_i(t_i)\big) \subseteq \mathsf{SC}\big(\mathsf{G}_j(t_j)\big)$ or $\mathsf{SC}\big(\mathsf{G}_j(t_j)\big) \subseteq \mathsf{SC}\big(\mathsf{G}_i(t_i)\big)$.*

Proof. Recall that $\mathsf{SB}\big(\mathsf{G}_i(t)\big)$ denotes the tip block of the stable main chain node i observes at time t. We first show that $\mathsf{SB}\big(\mathsf{G}_i(t)\big)$ is a stable block of graph $\mathsf{G}_i(t)$. In fact, by the definition of stable main chain in D11, $\mathsf{SB}\big(\mathsf{G}_i(t)\big)$

can be represented as

$$\mathsf{SB}\big(\mathsf{G}_i(t)\big) = \underset{B \in \mathsf{G}_i(t)}{\arg\max}\, \mathsf{h}\big(\mathsf{lsb}(B)\big). \tag{17}$$

For any $B \in \mathsf{G}_i(t)$, let $\mathsf{G}_i^B(t)$ denote the induced graph which consists of all blocks included by B. By Theorem 1, $\mathsf{lsb}(B)$ is a stable block of $\mathsf{G}_i^B(t)$. For any graph G^* such that $\mathsf{G}_i(t) \subseteq \mathsf{G}^*$, we have $\mathsf{G}_i^B(t) \subseteq \mathsf{G}_i(t) \subseteq \mathsf{G}^*$. It follows that $\mathsf{lsb}(B)$ is on the main chain of G^*. Thus, $\mathsf{lsb}(B)$ is a stable block of $\mathsf{G}_i(t)$. Therefore, according to the definition in (17), $\mathsf{SB}\big(\mathsf{G}_i(t)\big)$ is a stable block of $\mathsf{G}_i(t)$.

In order to prove that either $\mathsf{SC}\big(\mathsf{G}_i(t_i)\big) \subseteq \mathsf{SC}\big(\mathsf{G}_j(t_j)\big)$ or $\mathsf{SC}\big(\mathsf{G}_j(t_j)\big) \subseteq \mathsf{SC}\big(\mathsf{G}_i(t_i)\big)$ holds, it is equivalent to show that $\mathsf{SB}\big(\mathsf{G}_i(t_i)\big) \xrightarrow{b} \mathsf{SB}\big(\mathsf{G}_j(t_j)\big)$ or $\mathsf{SB}\big(\mathsf{G}_j(t_j)\big) \xrightarrow{b} \mathsf{SB}\big(\mathsf{G}_i(t_i)\big)$. In fact, by Assumption A6, there exists some time t_j^* such that $\mathsf{G}_i(t_i) \subseteq \mathsf{G}_j(t_j^*)$. Let $T = \max\{t_j, t_j^*\}$. We have both $\mathsf{G}_i(t_i) \subseteq \mathsf{G}_j(T)$ and $\mathsf{G}_j(t_j) \subseteq \mathsf{G}_j(T)$. Since $\mathsf{SB}\big(\mathsf{G}_i(t_i)\big)$ is a stable block of $\mathsf{G}_i(t_i)$, it follows that $\mathsf{SB}\big(\mathsf{G}_i(t_i)\big)$ is on the main chain of $\mathsf{G}_j(T)$. Similarly, $\mathsf{SB}\big(\mathsf{G}_j(t_j)\big)$ is on the main chain of $\mathsf{G}_j(T)$. Therefore, due to the uniqueness of the main chain, we have either $\mathsf{SB}\big(\mathsf{G}_i(t_i)\big) \xrightarrow{b} \mathsf{SB}\big(\mathsf{G}_j(t_j)\big)$ or $\mathsf{SB}\big(\mathsf{G}_j(t_j)\big) \xrightarrow{b} \mathsf{SB}\big(\mathsf{G}_i(t_i)\big)$. It completes the proof of Theorem 2. □

4.4 Liveness

If the block order is eventually determined, the following two requirements need to be met: 1) Each block will be included by some block on the stable main chain; and 2) the stable main chain will keep growing. Assume the former has been taken care of by the parent selection mechanism, e.g. each new block must reference all tip blocks in the local graph. To show the liveness property of our consensus algorithm, it remains to prove that each node can expand its stable main chain within finite time.

Recall that $\mathsf{G}_a(t)$ denotes the graph node a observes at time t. Given any deterministic function $f : \mathsf{G} \to \mathbb{R}$, we model $\{f\big(\mathsf{G}_a(t)\big) : t \geq 0\}$ as a stochastic process which is defined on a common probability space $(\Omega, \mathcal{F}, \mathsf{P})$, where Ω is a sample space, $\mathcal{F}$ is a σ-algebra, and P is a probability measure. The randomness comes from four different sources. The first is the parent selection mechanism, i.e., each witness may choose parents for his newly prepared block in some random manner. The second is the time when new blocks are issued. We assume that the blocks an honest witness prepares are distributed across time according to a homogeneous Poisson point process (p.p.p.) with intensity λ.[2] Here, in order to prepare a new block, an honest witness needs to select parents according to Assumptions A1 and A2. But the block does not need to satisfy Assumptions A3 and A4. In addition, the prepared blocks that also satisfy Assumptions A3 and A4 will be issued and propagated through the network. The only restriction we impose on malicious witnesses is that each malicious witness can only issue at most $X_{\max}$ blocks in unit time. The third is the randomness in the hash value of a block. We assume that any block among M blocks can have the largest hash value with equal probability $\frac{1}{M}$. The last origin of randomness is the transmission delay. By the partial asynchrony assumption in A6, let D denote the delay diameter of the network. Let $\{\mathcal{F}_t : t \geq 0\}$ denote an increasing family of sub-σ-algebras of $\mathcal{F}$, where $\mathcal{F}_t$ contains the information of all blocks that are prepared (no matter issued or not) up to time t. It is obvious that $\{f\big(\mathsf{G}_a(t)\big) : t \geq 0\}$ is adapted to the filtration $\{\mathcal{F}_t : t \geq 0\}$.

For any node n, we use $\mathsf{B}_n(t)$ denote the best (tip) block of graph $\mathsf{G}_n(t)$. We assume $\mathsf{ep}\big(\mathsf{B}_a(t)\big) = i$. The following Lemma 4 shows that $\mathsf{h}\big(\mathsf{SB}\big(\mathsf{G}_a(t)\big)\big)$ is either within $\mathcal{I}_i$ or the smallest number in $\mathcal{I}_{i+1}$.

Lemma 4. *For any graph $\mathsf{G}_a(t)$ such that $\mathsf{ep}\big(\mathsf{B}_a(t)\big) = i$, we have either $\mathsf{h}\big(\mathsf{SB}\big(\mathsf{G}_a(t)\big)\big) \in \mathcal{I}_i$ or $\mathsf{h}\big(\mathsf{SB}\big(\mathsf{G}_a(t)\big)\big) = \min\{x : x \in \mathcal{I}_{i+1}\}$.*

Proof. Assume $\mathsf{h}\big(\mathsf{SB}\big(\mathsf{G}_a(t)\big)\big) \in \mathcal{I}_j$. By the definition of $\mathsf{SB}\big(\mathsf{G}_a(t)\big)$ in D11, and the assumption that $\mathsf{ep}\big(\mathsf{B}_a(t)\big) = i$, i.e., $\mathsf{h}\big(\mathsf{lsb}\big(\mathsf{bp}\big(\mathsf{B}_a(t)\big)\big)\big) \in \mathcal{I}_i$., we have $j \geq i$. Let $B^* \in \mathsf{G}_a(t)$ denote the block such that $\mathsf{lsb}(B^*) = \mathsf{SB}\big(\mathsf{G}_a(t)\big)$. Since $\mathsf{B}_a(t)$ is the best block of $\mathsf{G}_a(t)$, we have $\mathsf{ep}(B^*) \leq \mathsf{ep}\big(\mathsf{B}_a(t)\big) = i$. Thus, there exists a $k \leq i$ such that $\mathsf{ep}(B^*) = k$. It implies that $\mathsf{h}\big(\mathsf{lsb}\big(\mathsf{bp}(B^*)\big)\big) \in \mathcal{I}_k$. According to how last stable block is determined in D10, we have $\mathsf{h}\big(\mathsf{SB}\big(\mathsf{G}_a(t)\big)\big) = \mathsf{h}\big(\mathsf{lsb}(B^*)\big)$ is either within $\mathcal{I}_k$ or equal to the minimum number in $\mathcal{I}_{k+1}$. Together with $\mathsf{h}\big(\mathsf{SB}\big(\mathsf{G}_a(t)\big)\big) \in \mathcal{I}_j$ for $j \geq i$, we have either $\mathsf{h}\big(\mathsf{SB}\big(\mathsf{G}_a(t)\big)\big) \in \mathcal{I}_i$ or $\mathsf{h}\big(\mathsf{SB}\big(\mathsf{G}_a(t)\big)\big) = \min\{x : x \in \mathcal{I}_{i+1}\}$. It completes the proof of Lemma 4. $\square$

In the following, we assume that the number of witnesses in each set $\mathcal{W}_i$ is upper bounded by a fixed number $N_{\max}$, i.e., $N_i \leq N_{\max}$. Let $\mathcal{E}(t, w^i)$ denote the event where no block is prepared by honest witnesses from $\mathcal{W}_i$ in time intervals $(t, t+D]$ and $(t+2D, t+3D]$, and only one honest witness from $\mathcal{W}_i$, i.e., w^i prepares a block in time interval $(t+D, t+2D]$. Here, we use the subscript i in w^i to denote that this witness is from set $\mathcal{W}_i$. According

[2] The homogeneous p.p.p. model is assumed here to facilitate analysis. Similar proof can be applied to non-homogeneous cases.

to our homogeneous p.p.p. assumption, the probability of $\mathcal{E}(t, w^i)$ can be evaluated as follows:

$$\lambda D e^{-\lambda D}\left(e^{-\lambda D}\right)^{K_i^h-1}\cdot e^{-2\lambda D K_i^h} = \lambda D e^{-3\lambda D K_i^h} \geq \lambda D e^{-3\lambda D N_{\max}} \triangleq \alpha, \quad (18)$$

where K_i^h denotes the number of honest witnesses in $\mathcal{W}_i$, and the last inequality is due to $K_i^h \leq N_i \leq N_{\max}$. Note that $0 < \alpha < 1$. We define $M_j = N_j - K_j + 1$ and $L_j = (3K_j - 1)M_j$ for any $j \in \mathbb{N}$. In the following, we analyze the two cases stated in Lemma 4 separately. The results for the first case are stated in Lemma 5 below.

Lemma 5. *For any $\mathsf{G}_a(t)$ such that $\mathsf{ep}\big(\mathsf{B}_a(t)\big) = i$ and $\mathsf{h}\big(\mathsf{SB}\big(\mathsf{G}_a(t)\big)\big) \in \mathcal{I}_i$, let $\mathcal{E}_1(t,i)$ denote the event where the stable main chain of $\mathsf{G}_a(t)$ is extended during time interval $\big(t, t+3L_iD\big]$. There exists an $\epsilon_1 > 0$ which is independent of t and i such that $\mathsf{P}\left(\mathcal{E}_1(t,i)\right) > \epsilon_1$.*

Proof. Let time interval $\big(t, t+3L_iD\big]$ be composed of $3K_i - 1$ frames, where the m-th frame, $1 \leq m \leq 3K_i - 1$, represents the time interval $\big(t+3(m-1)M_iD, t+3mM_iD\big]$. Each frame consists of M_i non-overlapping time intervals of length $3D$ each, called slots. Consider the following event sequence $\mathcal{S}$: event $\mathcal{E}\big(t+3(n-1)D, w_n^i\big)$ happens in the n-th slot for all $n = 1, 2, \cdots, L_i$. Here, w_n^i is chosen such that he is different from the witnesses in $\mathcal{W}_i$ who have issued a block among the last $K_i - 1$ blocks in the main chain of graph $\mathsf{G}_a\big(t+3(n-1)D\big)$.

We will show that there exists some $\beta > 0$ such that $\mathsf{P}\left(\mathcal{E}_1(t,i) \mid \mathcal{S}\right) > \beta$. The proof is carried out through two steps. In the first step, we show that in any frame, the probability that the stable main chain of $\mathsf{G}_a(t)$ is extended or at least one block prepared by an honest witness from $\mathcal{W}_i$ is successfully issued (i.e., satisfies Assumptions A3 and A4) is lower bounded by some $\gamma > 0$. The second step is to show that $\mathcal{E}_1(t,i)$ will happen given that there are at least $3K_i-1$ issued blocks by honest witnesses from $\mathcal{W}_i$ in time interval $(t, t+3L_iD]$. These two steps are analyzed in the following Lemma 6 and Lemma 7, respectively.

Lemma 6. *For any $m = 1, 2, \cdots, 3K_i - 1$, let $\mathcal{E}_m$ denote the event where $\mathsf{SC}\big(\mathsf{G}_a(t)\big) \subsetneq \mathsf{SC}\big(\mathsf{G}_a(t+3mM_iD)\big)$ or at least one block prepared by honest witnesses from $\mathcal{W}_i$ in the m-th frame is successfully issued. There exists $\gamma > 0$ such that*

$$\mathsf{P}\left(\mathcal{E}_m \mid \mathcal{S}, \mathcal{E}_{1,2,\cdots,m-1}\right) > \gamma, \quad (19)$$

where $\mathcal{E}_{1,2,\cdots,m-1}$ denotes the event sequence where $\mathcal{E}_s$ happens for all $s = 1, 2, \cdots, m-1$.

Proof of Lemma 6. We define the following terms for all $n = 0, 1, \cdots, L_i$. Define $l_n = \mathsf{lv}\big(\mathsf{B}_a(t+3nD)\big)$. Let $\mathsf{G}_{w_n^i}(\tau_n^-)$ denote w_n^i's local graph right before he prepares his new block at time τ_n. Recall that $\mathsf{B}_{w_n^i}(\tau_n^-)$ is the best (tip) block of $\mathsf{G}_{w_n^i}(\tau_n^-)$. We use $\mathcal{E}_{n,0}$ to denote the event where $\mathcal{E}\big(t+3(n-1)D, w_n^i\big)$ happens, the block prepared by witness w_n^i is not issued, $\mathsf{ep}\big(\mathsf{B}_{w_n^i}(\tau_n^-)\big) = i$ and $\mathsf{lv}\big(\mathsf{B}_{w_n^i}(\tau_n^-)\big) \geq l_{n-1}+1$. And let $\mathcal{E}_{n,1}$ denote the complement of $\mathcal{E}_{n,0}$ in $\mathcal{E}\big(t+3(n-1)D, w_n^i\big)$.

We focus on the m-th frame. For any $n = (m-1)M_i, \cdots, mM_i$, let $\mathcal{S}_n$ denote the event where $\mathcal{S}$ and $\mathcal{E}_{1,2,\cdots,m-1}$ happen, and the event sequence $\mathcal{E}_{(m-1)M_i+1,0}, \cdots, \mathcal{E}_{n,0}$ happens as well. We have

$$\mathsf{P}\left(\mathcal{E}_m \mid \mathcal{S}, \mathcal{E}_{1,2,\cdots,m-1}\right) = \mathsf{P}\left(\mathcal{E}_m \mid S_{(m-1)M_i}\right), \tag{20}$$

and for $n = (m-1)M_i+1, \cdots, mM_i$,

$$\begin{aligned} &\mathsf{P}\left(\mathcal{E}_m \mid \mathcal{S}_{n-1}\right) \\ =&\mathsf{P}\left(\mathcal{E}_m \mid \mathcal{S}_n\right)\mathsf{P}\left(\mathcal{E}_{n,0} \mid \mathcal{S}_{n-1}\right) + \\ &\mathsf{P}\left(\mathcal{E}_m \mid \mathcal{S}_{n-1}, \mathcal{E}_{n,1}\right)\mathsf{P}\left(\mathcal{E}_{n,1} \mid \mathcal{S}_{n-1}\right). \end{aligned} \tag{21}$$

Since $\mathcal{S}_{n-1}$ contains event $\mathcal{E}\big(t+3(n-1)D, w_n^i\big)$, we have

$$\begin{aligned} &\mathsf{P}\left(\mathcal{E}_{n,0} \mid \mathcal{S}_{n-1}\right) + \mathsf{P}\left(\mathcal{E}_{n,1} \mid \mathcal{S}_{n-1}\right) \\ =&\mathsf{P}\left(\mathcal{E}\big(t+3(n-1)D, w_n^i\big) \mid \mathcal{S}_{n-1}\right) = 1. \end{aligned} \tag{22}$$

We first claim that for all $n = (m-1)M_i+1, \cdots, mM_i$,

$$\mathsf{P}\left(\mathcal{E}_m \mid \mathcal{S}_{n-1}, \mathcal{E}_{n,1}\right) > \gamma, \tag{23}$$

where $\gamma = \frac{1}{1+X_{\max}(N_{\max}+3)D}$. In fact, if $\mathcal{E}_{n,1}$ happens, it will fall into one of the following three cases:

1) The block w_n^i prepares is successfully issued;

2) $\mathsf{ep}\big(\mathsf{B}_{w_n^i}(\tau_n^-)\big) > i$;

3) $\mathsf{ep}\big(\mathsf{B}_{w_n^i}(\tau_n^-)\big) = i$ and $\mathsf{lv}\big(\mathsf{B}_{w_n^i}(\tau_n^-)\big) \leq l_{n-1}$.

For case 1), $\mathcal{E}_m$ happens. For case 2), since $\mathsf{G}\big(\mathsf{B}_{w_n^i}(\tau_n^-)\big) \subseteq \mathsf{G}_a(t+3mM_iD)$, we have $\mathsf{ep}\big(\mathsf{B}_a(t+3mM_iD)\big) > i$, which leads to $\mathsf{h}\big(\mathsf{SB}\big(\mathsf{G}_a(t+3mM_iD)\big)\big) \in \mathcal{I}_j$ with $j > i$. Thus, $\mathsf{SB}\big(\mathsf{G}_a(t)\big) \neq \mathsf{SB}\big(\mathsf{G}_a(t+3mM_iD)\big)$, i.e., $\mathcal{E}_m$ happens. For case 3), since $\mathsf{G}_a\big(t+3(n-1)D\big) \subseteq \mathsf{G}\big(\mathsf{B}_{w_n^i}(\tau_n^-)\big)$, we have $\mathsf{ep}\big(\mathsf{B}_a(t+3(n-1)D)\big) = i$ and $\mathsf{lv}\big(\mathsf{B}_{w_n^i}(\tau_n^-)\big) \geq l_{n-1}$. Thus, $\mathsf{lv}\big(\mathsf{B}_{w_n^i}(\tau_n^-)\big) = l_{n-1}$. It follows that $\mathsf{B}_{w_n^i}(\tau_n^-)$ could be either $\mathsf{B}_a\big(t+3(n-1)D\big)$ or any other block with level l_{n-1}. Since no honest witness from $\mathcal{W}_i$ will issue a block in $\big(t+3(n-1)D, \tau_n\big)$, the number of candidates for $\mathsf{B}_{w_n^i}(\tau_n^-)$ is at most

$$1 + (N_i - K_i) \cdot X_{\max} \cdot \big(\tau_n - t - 3(n-1)D\big) \overset{(a)}{<} 1 + 3X_{\max} M_i D \overset{(b)}{<} \frac{1}{\gamma}, \quad (24)$$

where (a) is due to $M_i = N_i - K_i + 1 > N_i - K_i$ and $\tau_n \leq t + 3nD$, and (b) is by the fact that $M_i = N_i - K_i + 1 = \lceil \frac{1}{3} N_i \rceil < \frac{1}{3} N_{\max} + 1$. It follows that the probability of $\mathsf{B}_{w_n^i}(\tau_n^-) = \mathsf{B}_a\big(t + 3(n-1)D\big)$ is the same as the probability that the hash value of $\mathsf{B}_a\big(t + 3(n-1)D\big)$ is the largest among those of all candidates for $\mathsf{B}_{w_n^i}(\tau_n^-)$, which is greater than γ by (24). According to how w_n^i is selected, the block prepared by w_n^i will satisfy Assumption A4 if $\mathsf{B}_{w_n^i}(\tau_n^-) = \mathsf{B}_a\big(t + 3(n-1)D\big)$. In addition, if $\mathsf{h}\big(\mathsf{lsb}\big(\mathsf{B}_{w_n^i}(\tau_n^-)\big)\big) \in \mathcal{I}_k$ with $k > i$, the stable main chain of $\mathsf{G}_a(t)$ is extended, i.e., $\mathcal{E}_m$ happens. If $\mathsf{h}\big(\mathsf{lsb}\big(\mathsf{B}_{w_n^i}(\tau_n^-)\big)\big) \in \mathcal{I}_i$, it follows that the block prepared by w_n^i will satisfy Assumption A3. In sum, by combining the results for all three cases, the conditional probability of $\mathcal{E}_m$ given that $\mathcal{S}_{n-1}$ and $\mathcal{E}_{n,1}$ happen is larger than γ, which completes the proof of (23).

Next, we show that

$$\mathsf{P}\left(\mathcal{E}_{mM_i,0} \mid \mathcal{S}_{mM_i-1}\right) = 0. \quad (25)$$

We prove it by contradiction. Suppose $\mathcal{E}_{mM_i,0}$ can still happen if $\mathcal{S}_{mM_i-1}$ happens. By the definition $\mathcal{S}_{mM_i-1}$ and $\mathcal{E}_{mM_i,0}$, we have $\mathsf{ep}\big(\mathsf{B}_{w_n^i}(\tau_n^-)\big) = i$ and $\mathsf{lv}\big(\mathsf{B}_{w_n^i}(\tau_n^-)\big) \geq l_{n-1} + 1$ for all $n = (m-1)M_i + 1, \cdots, mM_i$. For all $n = (m-1)M_i + 1, \cdots, mM_i - 1$, since $\mathsf{G}\big(\mathsf{B}_{w_n^i}(\tau_n^-)\big) \subseteq \mathsf{G}_a(t + 3nD) \subseteq \mathsf{G}\big(\mathsf{B}_{w_{n+1}^i}(\tau_{n+1}^-)\big)$, we have $\mathsf{ep}\big(\mathsf{B}_a(t + 3nD)\big) = i$ and $\mathsf{lv}\big(\mathsf{B}_{w_n^i}(\tau_n^-)\big) \leq l_n$. It follows that $l_n \geq l_{n-1} + 1$ for all $n = (m-1)M_i + 1, \cdots, mM_i - 1$. Therefore, we have

$$\mathsf{lv}\big(\mathsf{B}_{w_{mM_i}^i}(\tau_{mM_i}^-)\big) \geq l_{mM_i-1} + 1 \geq l_{(m-1)M_i} + M_i. \quad (26)$$

However, none of the honest witnesses in $\mathcal{W}_i$ can contribute to the growth of l_n, since none of the blocks prepared by those witnesses within the m-th frame are successfully issued. It implies that

$$\mathsf{lv}\big(\mathsf{B}_{w_{mM_i}^i}(\tau_{mM_i}^-)\big) \leq l_{(m-1)M_i} + (N_i - K_i) < l_{(m-1)M_i} + M_i. \quad (27)$$

A contradiction occurs between (26) and (27), which finishes the proof of (25).

In the following, we prove by induction that for all $n = (m-1)M_i + 1, \cdots, mM_i$,

$$\mathsf{P}\left(\mathcal{E}_m \mid \mathcal{S}_{n-1}\right) > \gamma. \tag{28}$$

We start from $n = mM_i$. From (21), we have

$$\begin{aligned}
&\mathsf{P}\left(\mathcal{E}_m \mid \mathcal{S}_{mM_i-1}\right) \\
&\overset{(a)}{\geq} \mathsf{P}\left(\mathcal{E}_m \mid \mathcal{S}_{mM_i}\right) \cdot 0 + \mathsf{P}\left(\mathcal{E}_m \mid \mathcal{S}_{mM_i-1}, \mathcal{E}_{mM_i,1}\right) \cdot 1 \\
&\overset{(b)}{>} \gamma,
\end{aligned} \tag{29}$$

where (a) is from (22) and (25), and (b) is by (23) for $n = mM_i$. Thus, (28) holds for $n = mM_i$. Suppose (28) holds for some $(m-1)M_i + 2 \leq n \leq mM_i$. From (21), we have

$$\begin{aligned}
&\mathsf{P}\left(\mathcal{E}_m \mid \mathcal{S}_{n-2}\right) \\
&= \mathsf{P}\left(\mathcal{E}_m \mid \mathcal{S}_{n-1}\right) \mathsf{P}\left(\mathcal{E}_{n-1,0} \mid \mathcal{S}_{n-2}\right) + \mathsf{P}\left(\mathcal{E}_m \mid \mathcal{S}_{n-2}, \mathcal{E}_{n-1,1}\right) \mathsf{P}\left(\mathcal{E}_{n-1,1} \mid \mathcal{S}_{n-2}\right) \\
&\overset{(a)}{>} \gamma \mathsf{P}\left(\mathcal{E}_{n-1,0} \mid \mathcal{S}_{n-2}\right) + \gamma \mathsf{P}\left(\mathcal{E}_{n-1,1} \mid \mathcal{S}_{n-2}\right) \\
&\overset{(b)}{=} \gamma,
\end{aligned} \tag{30}$$

where (a) is by our assumption that (28) holds for n and (23), and (b) is due to (22). Therefore, (28) also holds for $n-1$, which gives the desired result for induction.

Therefore, from (20) we have

$$\mathsf{P}\left(\mathcal{E}_m \mid \mathcal{S}, \mathcal{E}_{1,2,\cdots,m-1}\right) = \mathsf{P}\left(\mathcal{E}_m \mid \mathcal{S}_{(m-1)M_i}\right) > \gamma, \tag{31}$$

where the inequality is due to (28) for $n = (m-1)M_i + 1$. It competes the proof of Lemma 6.

Lemma 7. *We have* $\mathsf{P}\left(\mathcal{E}_1(t,i) \mid \mathcal{E}_h, \mathcal{S}\right) = 1$*, where* $\mathcal{E}_h$ *denotes the event where at least* $3K_i - 1$ *blocks are issued by honest witnesses from* $\mathcal{W}_i$ *in time interval* $(t, t + 3L_iD]$.

Proof of Lemma 7. Assume the first $3K_i - 1$ blocks issued by honest witnesses from $\mathcal{W}_i$ during $(t, t+3L_iD]$ happen at slot $n_s, s = 1, 2, \cdots, 3K_i - 1$, respectively. Let $\tau_{n_s} \in \left(t + 3(n_s - 1) + D, t + 3n_sD\right]$ denote the time when witness $w^i_{n_s}$ issues his new block B_{n_s}. Let $\mathsf{G}_{w^i_{n_s}}(\tau^-_{n_s}), \mathsf{G}_{w^i_{n_s}}(\tau^+_{n_s})$ denote $w^i_{n_s}$'s local graph right before and after he issues B_{n_s}, respectively. Since the block transmission delay is upper bounded by D, we have

$$\begin{aligned}\mathsf{G}_a\big(t+3(n_s-1)+D\big) &\subseteq \mathsf{G}_{w^i_{n_s}}(\tau^-_{n_s}) \subseteq \mathsf{G}_{w^i_{n_s}}(\tau^+_{n_s}) \\ &\subseteq \mathsf{G}_a\big(t+3n_sD\big) \subseteq \mathsf{G}_{w^i_{n_{s+1}}}(\tau^-_{n_{s+1}}),\end{aligned} \tag{32}$$

for all $s = 1, 2, \cdots, 3K_i - 2$. Thus, $\mathsf{ep}\big(\mathsf{B}_a(t+3n_sD)\big) = i$ for all $s = 1, 2, \cdots, 3K_i - 2$. In addition, by Assumption A2, B_{n_s} will extend the main chain of $\mathsf{G}_{w^i_{n_s}}(\tau^-_{n_s})$ to generate the main chain of $\mathsf{G}_{w^i_{n_s}}(\tau^+_{n_s})$. Therefore, $l_{n_s} \geq l_{n_s-1} + 1$ holds for all $s = 1, 2, \cdots, 3K_i - 2$. It follows that

$$l_{n_s} \geq l_0 + s, \tag{33}$$

for all $s = 1, 2, \cdots, 3K_i - 2$.

Let C_s denote the main chain of $\mathsf{G}_a(t+3n_sD)$ for all $s = 1, \cdots, 3K_i - 2$. Let $\tilde{B}_{K_i}$ denote the block in C_{K_i} but not in $\mathsf{G}_a(t)$ with the smallest height, i.e.,

$$\tilde{B}_{K_i} = \mathop{\arg\min}_{B \in \mathsf{C}_{K_i} \text{ and } B \notin \mathsf{G}_a(t)} \mathsf{h}(B). \tag{34}$$

We claim that $B_{n_s} \xrightarrow{b} \tilde{B}_{K_i}$ for all $s > K_i$. It is proved by contradiction. Suppose $r > K_i$ is the smallest number such that $B_{n_r} \xrightarrow{b} \tilde{B}_{K_i}$ does not hold. It is true that more than $N_i - K_i$ blocks from $\{B_{n_1}, \cdots, B_{n_{K_i}}\}$ are included in C_{K_i}. Otherwise, C_{K_i} will contain at most $N_i - K_i$ blocks from $\{B_{n_1}, \cdots, B_{n_{K_i}}\}$ and at most $N_i - K_i$ blocks from malicious witnesses in $\mathcal{W}_i$, which leads to

$$l_{n_{K_i}} \leq l_0 + (N_i - K_i) + (N_i - K_i) < l_0 + K_i, \tag{35}$$

where the last inequality is due to $K_i > \frac{2}{3}N_i$ from Assumption A5. It is contradictory to (33) for $s = K_i$. Since $B_{n_r} \xrightarrow{b} \tilde{B}_{K_i}$ does not hold, none of the blocks in $\{B_{n_1}, \cdots, B_{n_{K_i}}\}$ that are included in C_{K_i} will show on the main chain of $\mathsf{G}_{w^i_{n_r}}(\tau^-_{n_r})$. Therefore, the main chain of $\mathsf{G}_{w^i_{n_r}}(\tau^-_{n_r})$ will contain less than $K_i - (N_i - K_i) = 2K_i - N_i$ blocks from $\{B_{n_1}, \cdots, B_{n_{K_i}}\}$. In addition, it does not contain B_{n_s} for any $K_i < s < r$ since $B_{n_s} \xrightarrow{b} \tilde{B}_{K_i}$ by the definition of r. Furthermore, the main chain of $\mathsf{G}_{w^i_{n_r}}(\tau^-_{n_r})$ can contain at most $N_i - K_i$ blocks from malicious witnesses in $\mathcal{W}_i$. Therefore, we have

$$\mathsf{lv}\big(\mathsf{B}_{w^i_{n_r}}(\tau^-_{n_r})\big) < l_0 + (2K_i - N_i) + (N_i - K_i) = l_0 + K_i \leq l_{n_{r-1}}, \tag{36}$$

where the last inequality is by (33) and the fact that $r \geq K_i + 1$. Since $\mathsf{C}_{r-1} \subseteq \mathsf{G}_{w^i_{n_r}}(\tau^-_{n_r})$, (36) contradicts with the fact that $\mathsf{B}_{w^i_{n_r}}(\tau^-_{n_r})$ is the best block in graph $\mathsf{G}_{w^i_{n_r}}(\tau^-_{n_r})$. It competes the proof that $B_{n_s} \xrightarrow{b} \tilde{B}_{K_i}$ for all $s > K_i$.

For any block $B \in \mathsf{G}_a(t)$ such that $\tilde{B}_{K_i} \xrightarrow{b} B$, suppose $\tilde{B} \in \mathsf{G}_a(t + 3L_iD)$ satisfies $\tilde{B} \xrightarrow{b} B$ and $\tilde{B}_{K_i} \notin \mathsf{C}(B, \tilde{B})$. Let $\mathcal{T}$ denote the set of blocks that are added into $\mathsf{C}(B, \tilde{B})$ after time t. $\mathcal{T}$ does not contain blocks from $\{B_{n_1}, \cdots, B_{n_{K_i}}\}$ that are included in C_{K_i}, whose number is greater than $N_i - K_i$. In addition, $\mathcal{T}$ does not contain any block from $\{B_{n_{K_i+1}}, \cdots, B_{n_{3K_i-2}}\}$ since $B_{n_s} \xrightarrow{b} \tilde{B}_{K_i}$ for all $s > K_i$. Furthermore, there are at most $N_i - K_i$ malicious witnesses in $\mathcal{W}_i$ by Assumption A5. Thus, we have

$$\mathsf{lv}(\tilde{B}) < l_0 + (K_i - (N_i - K_i)) + (N_i - K_i) = l_0 + K_i. \tag{37}$$

Since $l_{n_{3K_i-2}} \geq l_0 + (3K_i - 2)$ by (33), we conclude that $l_{n_{3K_i-2}} > \mathsf{lv}(\tilde{B}) + 2(K_i - 1)$ holds. Similarly as in (37), it can be shown that $\tilde{B}_{K_i} \in \mathsf{C}_{3K_i-2}$. In fact, if $\tilde{B}_{K_i} \notin \mathsf{C}_{3K_i-2}$, we have $l_{n_{3K_i-2}} < l_0 + K_i$, which is contradictory to $l_{n_{3K_i-2}} \geq l_0 + (3K_i - 2)$. Therefore, the tip block of C_{3K_i-2}, i.e., $\mathsf{B}_a\big(t + 3n_{3K_i-2}D\big)$ satisfies the condition (2) with respect to any block $B \in \mathsf{G}_a(t)$ with $\tilde{B}_{K_i} \xrightarrow{b} B$. It follows that the stable main chain of $\mathsf{G}_a\big(t+3n_{3K_i-2}D\big)$ will contain $\tilde{B}_{K_i}$, which implies that the stable main chain of $\mathsf{G}_a(t)$ is extended during $(t, t + 3L_iD]$. It completes the proof of Lemma 7.

With the results in Lemma 6 and 7, we continue the proof of Lemma 5. Now, we have

$$\begin{aligned}
&\mathsf{P}\left(\mathcal{E}_1(t,i) \mid \mathcal{S}\right) \\
&\geq \mathsf{P}\left(\mathcal{E}_{1,2,\cdots,3K_i-1} \mid \mathcal{S}\right) \cdot \mathsf{P}\left(\mathcal{E}_1(t,i) \mid \mathcal{S}, \mathcal{E}_{1,2,\cdots,3K_i-1}\right) \\
&\overset{(a)}{\geq} \prod_{m=1}^{3K_i-1} \mathsf{P}\left(\mathcal{E}_m \mid \mathcal{S}, \mathcal{E}_{1,2,\cdots,m-1}\right) \cdot 1 \\
&\overset{(b)}{>} \gamma^{3K_i-1} \overset{(c)}{>} \gamma^{3N_{\max}+5} \triangleq \beta > 0,
\end{aligned} \tag{38}$$

where (a) is by Lemma 7 because if $\mathcal{S}$ and $\mathcal{E}_{1,2,\cdots,3K_i-1}$ happen, either the stable main chain of $\mathsf{G}_a(t)$ is extended during $(t, t+3L_iD]$ or at least $3K_i-1$ blocks are issued by honest witnesses from $\mathcal{W}_i$ during $(t, t + 3L_iD)$, i.e., $\mathcal{E}_h$ happens, (b) is by Lemma 6, and (c) is due to $K_i = \lfloor \frac{2}{3}N_i \rfloor + 1 < \frac{2}{3}N_{\max} + 2$. In addition, since $K_i = \lfloor \frac{2}{3}N_i \rfloor + 1$, we have $M_i = N_i - K_i + 1 = \lceil \frac{1}{3}N_i \rceil$, which leads to

$$
\begin{aligned}
L_i &= (3K_i - 2)M_i \\
&< \left(3\left(\frac{2}{3}N_i + 2\right) - 2\right)\left(\frac{1}{3}N_i + 1\right) \\
&\leq \frac{2}{3}(N_{\max} + 2)(N_{\max} + 3),
\end{aligned} \tag{39}
$$

where the last inequality is due to $N_i \leq N_{\max}$. Thus, a lower bound on the probability of $\mathcal{S}$ is

$$
\mathsf{P}(\mathcal{S}) \overset{(a)}{\geq} \alpha^{L_i} \overset{(b)}{>} \alpha^{\frac{2}{3}(N_{\max}+2)(N_{\max}+3)}, \tag{40}
$$

where (a) is due to (18), and (b) is by the fact that $0 < \alpha < 1$ and (39). Therefore, by (38) and (40), we have

$$
\mathsf{P}(\mathcal{E}_1(t,i)) \geq \mathsf{P}(\mathcal{E}_1(t,i) \mid \mathcal{S}) \cdot \mathsf{P}(\mathcal{S}) > \beta\alpha^{\frac{2}{3}(N_{\max}+2)(N_{\max}+3)} \triangleq \epsilon_1 > 0. \tag{41}
$$

It completes the proof of Lemma 5. □

In the following Lemma 8, we analyze the second case in Lemma 4 using a similar idea as in Lemma 5.

Lemma 8. *For any $\mathsf{G}_a(t)$ such that $\mathsf{ep}\big(\mathsf{B}_a(t)\big) = i$ and $\mathsf{h}\big(\mathsf{SB}\big(\mathsf{G}_a(t)\big)\big) = \min\{x : x \in \mathcal{I}_{i+1}\}$, let $\mathcal{E}_2(t,i)$ denote the event where the stable main chain of $\mathsf{G}_a(t)$ is extended during time interval $\big(t, t + 6L_iD + 3L_{i+1}D\big]$. There exists an $\epsilon_2 > 0$ which is independent of t and i such that $\mathsf{P}(\mathcal{E}_2(t,i)) > \epsilon_2$.*

Proof. Let time interval $\big(t, t + 6L_iD\big]$ be composed of $3K_i - 1$ frames, where the m-th frame, $1 \leq m \leq 3K_i - 1$, represents the time interval $\big(t + 6(m-1)M_iD, t + 6mM_iD\big]$. Each frame consists of M_i non-overlapping time intervals of length $6D$ each, called slots. Each slot contains two sub-slots of length $3D$ each. Consider the following event sequence $\tilde{\mathcal{S}}$: In the n-th slot for all $n = 1, 2, \cdots, L_i$, event $\mathcal{E}\big(t + 6(n-1)D, w_n^i\big)$ happens in the first sub-slot, and event $\mathcal{E}\big(t + (6n-3)D, w_n^{i+1}\big)$ happens in the second sub-slot. Here, w_n^i is chosen such that he is different from the witnesses in $\mathcal{W}_i$ who have issued a block among the last $K_i - 1$ blocks in the main chain of graph $\mathsf{G}_a\big(t + 6(n-1)D\big)$. Similarly, w_n^{i+1} is chosen such that he is different from the witnesses in $\mathcal{W}_{i+1}$ who have issued a block among the last $K_{i+1} - 1$ blocks in the main chain of graph $\mathsf{G}_a\big(t + (6n-3)D\big)$. We first show the following result which is similar to Lemma 6.

Lemma 9. *For any $m = 1, 2, \cdots, 3K_i - 1$, let $\tilde{\mathcal{E}}_m$ denote the event where $\mathsf{ep}\big(\mathsf{B}_a(t + 6mM_iD)\big) > i$ or at least one block prepared by honest witnesses from $\mathcal{W}_i$ or $\mathcal{W}_{i+1}$ in the m-th frame is successfully issued. There exists $\delta > 0$ such that*

$$\mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}, \tilde{\mathcal{E}}_{1,2,\cdots,m-1}\right) > \delta, \tag{42}$$

where $\tilde{\mathcal{E}}_{1,2,\cdots,m-1}$ denotes the event sequence where $\tilde{\mathcal{E}}_s$ happens for all $s = 1, 2, \cdots, m-1$.

Proof of Lemma 9. We define the following terms for all $n = 0, 1, \cdots, L_i$. Define $\bar{l}_n = \mathsf{lv}\big(\mathsf{B}_a(t + 6nD)\big)$. Let $\mathsf{G}_{w_n^i}(\tau_{n,i}^-)$ and $\mathsf{G}_{w_n^{i+1}}(\tau_{n,i+1}^-)$ denote w_n^i's and w_n^{i+1}'s local graph right before he prepares his new block at time $\tau_{n,i}$ and $\tau_{n,i+1}$, respectively. Recall that $\mathsf{B}_{w_n^i}(\tau_{n,i}^-)$ and $\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-)$ are the best (tip) block of $\mathsf{G}_{w_n^i}(\tau_{n,i}^-)$ and $\mathsf{G}_{w_n^{i+1}}(\tau_{n,i+1}^-)$, respectively. We use $\tilde{\mathcal{E}}_{n,0}$ to denote the event where events $\mathcal{E}\big(t + 6(n-1)D, w_n^i\big)$ and $\mathcal{E}\big(t + (6n - 3)D, w_n^{i+1}\big)$ happen, blocks prepared by witness w_n^i and w_n^{i+1} are not issued, and either $\mathsf{ep}\big(\mathsf{B}_{w_n^i}(\tau_{n,i}^-)\big) = i$, $\mathsf{lv}\big(\mathsf{B}_{w_n^i}(\tau_{n,i}^-)\big) \geq \bar{l}_{n-1} + 1$ or $\mathsf{ep}\big(\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-)\big) = i$, $\mathsf{lv}\big(\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-)\big) \geq \bar{l}_{n-1} + 1$ holds. And let $\tilde{\mathcal{E}}_{n,1}$ denote the complement of $\tilde{\mathcal{E}}_{n,0}$ in the union of $\mathcal{E}\big(t + 6(n-1)D, w_n^i\big)$ and $\mathcal{E}\big(t + (6n-3)D, w_n^{i+1}\big)$.

We focus on the m-th frame. For any $n = (m-1)M_i, \cdots, mM_i$, let $\tilde{\mathcal{S}}_n$ denote the event where $\tilde{\mathcal{S}}$ and $\tilde{\mathcal{E}}_{1,2,\cdots,m-1}$ happen, and the event sequence $\tilde{\mathcal{E}}_{(m-1)M_i+1,0}, \cdots, \tilde{\mathcal{E}}_{n,0}$ happens as well. We have

$$\mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}, \tilde{\mathcal{E}}_{1,2,\cdots,m-1}\right) = \mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}_{(m-1)M_i}\right), \tag{43}$$

and for $n = (m-1)M_i + 1, \cdots, mM_i$,

$$\begin{aligned} &\mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}_{n-1}\right) \\ =&\mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}_n\right)\mathsf{P}\left(\tilde{\mathcal{E}}_{n,0} \mid \tilde{\mathcal{S}}_{n-1}\right) + \\ &\mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}_{n-1}, \tilde{\mathcal{E}}_{n,1}\right)\mathsf{P}\left(\tilde{\mathcal{E}}_{n,1} \mid \tilde{\mathcal{S}}_{n-1}\right). \end{aligned} \tag{44}$$

Since $\tilde{\mathcal{S}}_{n-1}$ contains events $\mathcal{E}\big(t + 6(n-1)D, w_n^i\big)$ and $\mathcal{E}\big(t + (6n-3)D, w_n^{i+1}\big)$, we have

$$\begin{aligned} &\mathsf{P}\left(\tilde{\mathcal{E}}_{n,0} \mid \tilde{\mathcal{S}}_{n-1}\right) + \mathsf{P}\left(\tilde{\mathcal{E}}_{n,1} \mid \tilde{\mathcal{S}}_{n-1}\right) \\ =&\mathsf{P}\left(\mathcal{E}\big(t + 6(n-1)D, w_n^i\big), \mathcal{E}\big(t + (6n-3)D, w_n^{i+1}\big) \mid \tilde{\mathcal{S}}_{n-1}\right) \\ =&1. \end{aligned} \tag{45}$$

We first claim that for $n = (m-1)M_i + 1, \cdots, mM_i$,

$$\mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}_{n-1}, \tilde{\mathcal{E}}_{n,1}\right) > \delta, \tag{46}$$

where $\delta = \frac{1}{1+2X_{\max}(N_{\max}+3)D}$. In fact, if $\tilde{\mathcal{E}}_{n,1}$ happens, it will fall into one of the following three cases:

1) The block w_n^i or w_n^{i+1} prepares is successfully issued;
2) $\mathsf{ep}\big(\mathsf{B}_{w_n^i}(\tau_{n,i}^-)\big) > i$ or $\mathsf{ep}\big(\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-)\big) > i$;
3) $\mathsf{ep}\big(\mathsf{B}_{w_n^i}(\tau_{n,i}^-)\big) = \mathsf{ep}\big(\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-)\big) = i$ and $\mathsf{lv}\big(\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-)\big) \le \bar{l}_{n-1}$, $\mathsf{lv}\big(\mathsf{B}_{w_n^i}(\tau_{n,i}^-)\big) \le \bar{l}_{n-1}$.

For case 1), $\tilde{\mathcal{E}}_m$ happens. For the case 2), since $\mathsf{G}\big(\mathsf{B}_{w_n^i}(\tau_{n,i}^-)\big) \subseteq \mathsf{G}_a(t + 6nD)$ and $\mathsf{G}\big(\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-)\big) \subseteq \mathsf{G}_a(t+6nD)$, we have $\mathsf{ep}\big(\mathsf{B}_a(t+6nD)\big) > i$, which implies that $\mathcal{E}_m$ happens. For case 3), since $\mathsf{G}_a\big(t+6(n-1)D\big) \subseteq \mathsf{G}\big(\mathsf{B}_{w_n^i}(\tau_{n,i}^-)\big) \subseteq \mathsf{G}\big(\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-)\big)$, we have $\mathsf{ep}\big(\mathsf{B}_a(t+6(n-1)D)\big) = i$ and $\bar{l}_{n-1} \le \mathsf{lv}\big(\mathsf{B}_{w_n^i}(\tau_{n,i}^-)\big) \le \mathsf{lv}\big(\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-)\big)$. Therefore, $\mathsf{lv}\big(\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-)\big) = \mathsf{lv}\big(\mathsf{B}_{w_n^i}(\tau_{n,i}^-)\big) = \bar{l}_{n-1}$. It follows that $\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-)$ could be either $\mathsf{B}_a\big(t+6(n-1)D\big)$ or any other block with level $\bar{l}_{n-1}$. Since the block prepared by w_n^i is not issued, otherwise we will have $\mathsf{lv}\big(\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-)\big) > \bar{l}_{n-1}$, no honest witness from $\mathcal{W}_i$ will issue a block in time interval $\big(t+6(n-1)D, \tau_{n,i+1}\big)$. Thus, the number of candidates for $\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-)$ is at most

$$1 + (N_i - K_i)\cdot X_{\max}\cdot\big(\tau_{n,i+1} - t - 6(n-1)D\big) \overset{(a)}{<} 1 + 6X_{\max}M_iD \overset{(b)}{<} \frac{1}{\delta}, \tag{47}$$

where (a) is due to $M_i = N_i - K_i + 1 > N_i - K_i$ and $\tau_{n,i+1} \le t + 6nD$, and (b) is by the fact that $M_i = N_i - K_i + 1 = \left\lceil \frac{1}{3}N_i \right\rceil < \frac{1}{3}N_{\max} + 1$. It follows that the probability of $\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-) = \mathsf{B}_a\big(t+6(n-1)D\big)$ is the same as the probability that the hash value of $\mathsf{B}_a\big(t+6(n-1)D\big)$ is the largest among those of all candidates for $\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-)$, which is greater than δ by (47). Consider the following three cases for $\mathsf{h}\big(\mathsf{lsb}\big(\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-)\big)\big)$ given $\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-) = \mathsf{B}_a\big(t+6(n-1)D\big)$.

a. $\mathsf{h}\big(\mathsf{lsb}\big(\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-)\big)\big) \in \mathcal{I}_i$: Given $\mathsf{B}_{w_n^{i+1}}(\tau_{n,i+1}^-) = \mathsf{B}_a\big(t+6(n-1)D\big)$, we have $\mathsf{B}_{w_n^i}(\tau_{n,i}^-) = \mathsf{B}_a\big(t+6(n-1)D\big)$ and $\mathsf{h}\big(\mathsf{lsb}\big(\mathsf{B}_{w_n^i}(\tau_{n,i}^-)\big)\big) \in \mathcal{I}_i$ as well. According to how w_n^i is selected, the block prepared by w_n^i will satisfy Assumptions A3 and A4. Thus, this block is successfully issued, i.e., $\tilde{\mathcal{S}}_m$ happens.

b. $\mathsf{h}\big(\mathsf{lsb}\big(\mathsf{B}_{w_n^{i+1}}(\tau^-_{n,i+1})\big)\big) \in \mathcal{I}_{i+1}$: According to how w_n^{i+1} is selected, the block prepared by w_n^{i+1} will satisfy Assumptions A3 and A4 given $\mathsf{B}_{w_n^{i+1}}(\tau^-_{n,i+1}) = \mathsf{B}_a\big(t+6(n-1)D\big)$. Thus, this block is successfully issued, i.e., $\tilde{\mathcal{S}}_m$ happens.

c. $\mathsf{h}\big(\mathsf{lsb}\big(\mathsf{B}_{w_n^{i+1}}(\tau^-_{n,i+1})\big)\big) \in \mathcal{I}_k$ with $k > i+1$: We have $\mathsf{ep}\big(\mathsf{B}_{w_n^{i+1}}(\tau^-_{n,i+1})\big) \geq k-1 > i$. It implies that $\tilde{\mathcal{S}}_m$ happens by case 2) we have analyzed above.

In sum, by combining the results above for all three cases, the probability that $\tilde{\mathcal{E}}_m$ happens is larger than δ, which completes the proof of (46).

Next, we show that

$$\mathsf{P}\left(\tilde{\mathcal{E}}_{mM_i,0} \mid \tilde{\mathcal{S}}_{mM_i-1}\right) = 0. \tag{48}$$

We prove it by contradiction. Suppose $\tilde{\mathcal{E}}_{mM_i,0}$ can still happen if $\tilde{\mathcal{S}}_{mM_i-1}$ happens. By the definition $\tilde{\mathcal{S}}_{mM_i-1}$ and $\tilde{\mathcal{E}}_{mM_i,0}$, we have either $\mathsf{ep}\big(\mathsf{B}_{w_n^i}(\tau^-_{n,i})\big) = i$, $\mathsf{lv}\big(\mathsf{B}_{w_n^i}(\tau^-_{n,i})\big) \geq \bar{l}_{n-1}+1$ or $\mathsf{ep}\big(\mathsf{B}_{w_n^{i+1}}(\tau^-_{n,i+1})\big) = i$, $\mathsf{lv}\big(\mathsf{B}_{w_n^{i+1}}(\tau^-_{n,i+1})\big) \geq \bar{l}_{n-1}+1$ holds for all $n = (m-1)M_i+1, \cdots, mM_i$. For all $n = (m-1)M_i + 1, \cdots, mM_i - 1$, we have

$$\begin{aligned}&\mathsf{G}_a(t+6(n-1)D) \subseteq \mathsf{G}_{w_n^i}(\tau^-_{n,i}) \subseteq \mathsf{G}_{w_n^{i+1}}(\tau^-_{n,i+1})\\ &\subseteq \mathsf{G}_a(t+6nD) \subseteq \mathsf{G}_{w_{n+1}^i}(\tau^-_{n+1,i}) \subseteq \mathsf{G}_{w_{n+1}^{i+1}}(\tau^-_{n+1,i+1}).\end{aligned} \tag{49}$$

It follows that $\mathsf{ep}\big(\mathsf{B}_a(t+6nD)\big) = i$ and $\bar{l}_n \geq \bar{l}_{n-1}+1$ for all $n = (m-1)M_i+1, \cdots, mM_i-1$. Therefore, if $\mathsf{lv}\big(\mathsf{B}_{w_n^i}(\tau^-_{n,i})\big) \geq \bar{l}_{n-1}+1$ for $n = mM_i$, we have

$$\mathsf{lv}\big(\mathsf{B}_{w_{mM_i}^i}(\tau^-_{mM_i,i})\big) \geq \bar{l}_{mM_i-1}+1 \geq \bar{l}_{(m-1)M_i} + M_i. \tag{50}$$

However, none of the honest witnesses in $\mathcal{W}_i$ can contribute to the growth of $\bar{l}_n$, since none of the blocks prepared by those witnesses within the m-th frame are successfully issued. It implies that

$$\mathsf{lv}\big(\mathsf{B}_{w_{mM_i}^i}(\tau^-_{mM_i,i})\big) \leq \bar{l}_{(m-1)M_i} + (N_i - K_i) < \bar{l}_{(m-1)M_i} + M_i. \tag{51}$$

A contradiction occurs between (50) and (51). Similarly, we will have a contradiction if $\mathsf{lv}\big(\mathsf{B}_{w_n^{i+1}}(\tau^-_{n,i+1})\big) \geq \bar{l}_{n-1}+1$ for $n = mM_i$. It finishes the proof of (48).

In the following, we prove by induction that for all $n = (m-1)M_i + 1, \cdots, mM_i$,

$$\mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}_{n-1}\right) > \delta. \tag{52}$$

We start from $n = mM_i$. From (44), we have

$$\begin{aligned}
&\mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}_{mM_i-1}\right) \\
\overset{(a)}{\geq}\,& \mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}_{mM_i}\right) \cdot 0 + \mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}_{mM_i-1}, \mathcal{E}_{mM_i,1}\right) \cdot 1 \\
\overset{(b)}{>}\,& \delta,
\end{aligned} \tag{53}$$

where (a) is from (45) and (48), and (b) is by (46) for $n = mM_i$. Thus, (52) holds for $n = mM_i$. Suppose (52) holds for some $(m-1)M_i + 2 \leq n \leq mM_i$. From (44), we have

$$\begin{aligned}
&\mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}_{n-2}\right) \\
=\,& \mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}_{n-1}\right) \mathsf{P}\left(\tilde{\mathcal{E}}_{n-1,0} \mid \tilde{\mathcal{S}}_{n-2}\right) + \mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}_{n-2}, \tilde{\mathcal{E}}_{n-1,1}\right) \mathsf{P}\left(\tilde{\mathcal{E}}_{n-1,1} \mid \tilde{\mathcal{S}}_{n-2}\right) \\
\overset{(a)}{>}\,& \delta \mathsf{P}\left(\tilde{\mathcal{E}}_{n-1,0} \mid \tilde{\mathcal{S}}_{n-2}\right) + \delta \mathsf{P}\left(\tilde{\mathcal{E}}_{n-1,1} \mid \tilde{\mathcal{S}}_{n-2}\right) \\
\overset{(b)}{=}\,& \delta,
\end{aligned} \tag{54}$$

where (a) is by our assumption that (52) holds for n and (46), and (b) is due to (45). Therefore, (52) also holds for $n-1$, which gives the desired result for induction.

Therefore, from (43) we have

$$\mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}, \tilde{\mathcal{E}}_{1,2,\cdots,m-1}\right) = \mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}_{(m-1)M_i}\right) > \delta, \tag{55}$$

where the inequality is due to (52) for $n = (m-1)M_i + 1$. It competes the proof of Lemma 9.

We continue the proof of Lemma 8. Given that events $\tilde{\mathcal{S}}$ and $\tilde{\mathcal{E}}_{1,2,\cdots,3K_i-1}$ happen, one of the following three cases will happen:

a. There exists $m_0 \in \{1, 2, \cdots, 3K_i - 1\}$ such that $\mathsf{ep}\big(\mathsf{B}_a(t + 6m_0M_iD)\big) > i$;

b. There exists $m_1 \in \{1, 2, \cdots, 3K_i - 1\}$ such that some block prepared by an honest witness from $\mathcal{W}_{i+1}$ is successfully issued in the m_1-th frame;

c. For all $m \in \{1, 2, \cdots, 3K_i - 1\}$, at least one block by an honest witness from $\mathcal{W}_i$ is successfully issued in the m-th frame.

For the first two cases, we have $\mathsf{ep}\big(\mathsf{G}_a(t+6L_iD)\big) = k > i$. If $k > i+1$, the stable main chain of $\mathsf{G}_a(t)$ is extended during $(t, t+6L_iD]$, i.e., $\mathcal{E}_2(t,i)$ happens. If $k = i+1$, by Lemma 4, we have either $\mathsf{h}\big(\mathsf{SB}\big(\mathsf{G}_a(t+6L_iD)\big)\big) \in \mathcal{I}_{i+1}$ or $\mathsf{h}\big(\mathsf{SB}\big(\mathsf{G}_a(t+6L_iD)\big)\big) = \min\{x : x \in \mathcal{I}_{i+2}\}$. If $\mathsf{h}\big(\mathsf{SB}\big(\mathsf{G}_a(t+6L_iD)\big)\big) = \min\{x : x \in \mathcal{I}_{i+2}\}$, the stable main chain of $\mathsf{G}_a(t)$ is extended during $(t, t+6L_iD]$, i.e., $\mathcal{E}_2(t,i)$ happens; if $\mathsf{h}\big(\mathsf{SB}\big(\mathsf{G}_a(t+6L_iD)\big)\big) \in \mathcal{I}_{i+1}$, by Lemma 5, we have $\mathsf{P}\left(\mathcal{E}_1(t+6L_iD, i+1)\right) > \epsilon_1$, i.e., the probability that the stable main chain of $\mathsf{G}_a(t+6L_iD)$ is extended during $(t+6L_iD, t+6L_iD+3L_{i+1}D]$ is larger than ϵ_1. In sum, given the first two cases, the probability that $\mathcal{E}_2(t,i)$ happens is larger than ϵ_1. For the last case, similarly as in Lemma 7, $\mathcal{E}_2(t,i)$ almost surely happens. The proof is omitted to avoid repetition. By combining the results for all three cases, we have

$$\mathsf{P}\left(\mathcal{E}_2(t,i) \mid \tilde{\mathcal{S}}, \tilde{\mathcal{E}}_{1,2,\cdots,3K_i-1}\right) > \epsilon_1. \tag{56}$$

Now, we have

$$\begin{aligned}
&\mathsf{P}\left(\mathcal{E}_2(t,i) \mid \tilde{\mathcal{S}}\right)\\
\geq &\,\mathsf{P}\left(\tilde{\mathcal{E}}_{1,2,\cdots,3K_i-1} \mid \tilde{\mathcal{S}}\right) \cdot \mathsf{P}\left(\mathcal{E}_2(t,i) \mid \tilde{\mathcal{S}}, \tilde{\mathcal{E}}_{1,2,\cdots,3K_i-1}\right)\\
\overset{(a)}{\geq} &\prod_{m=1}^{3K_i-1} \mathsf{P}\left(\tilde{\mathcal{E}}_m \mid \tilde{\mathcal{S}}, \tilde{\mathcal{E}}_{1,2,\cdots,m-1}\right) \cdot \epsilon_1\\
\overset{(b)}{>} &\,\epsilon_1 \delta^{3K_i-1} \overset{(c)}{>} \epsilon_1 \delta^{3N_{\max}+5},
\end{aligned} \tag{57}$$

where (a) is by (56), (b) is by Lemma 9, and (c) is due to $K_i = \lfloor \frac{2}{3}N_i \rfloor + 1 < \frac{2}{3}N_{\max} + 2$. In addition, a lower bound on the probability of $\tilde{\mathcal{S}}$ is

$$\mathsf{P}\left(\tilde{\mathcal{S}}\right) \overset{(a)}{\geq} \alpha^{2L_i} \overset{(b)}{>} \alpha^{\frac{4}{3}(N_{\max}+2)(N_{\max}+3)}, \tag{58}$$

where (a) is due to (18), and (b) is by the fact that $0 < \alpha < 1$ and (39). Therefore, by (57) and (58), we have

$$\begin{aligned}
\mathsf{P}\left(\mathcal{E}_2(t,i)\right) &\geq \mathsf{P}\left(\tilde{\mathcal{E}}_2(t,i) \mid \tilde{\mathcal{S}}\right) \cdot \mathsf{P}\left(\tilde{\mathcal{S}}\right)\\
&> \epsilon_1 \delta^{3N_{\max}+5} \alpha^{\frac{4}{3}(N_{\max}+2)(N_{\max}+3)} \triangleq \epsilon_2 > 0.
\end{aligned} \tag{59}$$

It completes the proof of Lemma 8. □

The liveness property of our consensus algorithm is stated and proved in the following Theorem 3.

Theorem 3. *For any $t_0 \geq 0$, let*

$$T = \min\{t \geq t_0 : \mathsf{SC}\big(\mathsf{G}_a(t_0)\big) \subsetneq \mathsf{SC}\big(\mathsf{G}_a(t)\big)\},$$

we have $\mathsf{E}\{T\} < \infty$.

Proof. It is easy to see that T is a stopping time with respect to filtration $\{\mathcal{F}_t : t \geq 0\}$. Let $\Delta = 6(N_{\max}+2)(N_{\max}+3)D$. For any $t \geq t_0$, we assume $\mathsf{ep}\big(\mathsf{B}_a(t)\big) = i$. From Lemma 5 and Lemma 8, we have

$$\mathsf{P}\left(\mathsf{SC}\big(\mathsf{G}_a(t)\big) \subsetneq \mathsf{SC}\big(\mathsf{G}_a(t + 6L_iD + 3L_{i+1}D)\big)\right) > \min(\epsilon_1, \epsilon_2) \triangleq \epsilon > 0. \quad (60)$$

Since $6L_iD + 3L_{i+1}D < \Delta$ from (39) and $\mathsf{SC}\big(\mathsf{G}_a(t_0)\big) \subseteq \mathsf{SC}\big(\mathsf{G}_a(t)\big)$, the following condition holds almost surely (a.s.):

$$\mathsf{P}\left(T \leq t + \Delta \mid \mathcal{F}_t\right) > \epsilon. \quad (61)$$

In the following, we prove that $\mathsf{E}\{T\} < \infty$. It is very similar to the "Awaiting the almost inevitable" in [12], Chapter 10.11. We first use induction to show that for all $k = 0, 1, 2, \cdots$,

$$\mathsf{P}\left(T > t_0 + k\Delta\right) \leq (1-\epsilon)^k. \quad (62)$$

It is obvious that (62) holds for $k = 0$ since $\mathsf{P}\left(T > t_0\right) = 1$. Now assume that (62) holds for some $k \geq 0$. Let $1_{\{\cdot\}}$ to denote the indicator function. We have

$$\begin{aligned}
&\mathsf{P}\left(T > t_0 + (k+1)\Delta\right) \\
=&\mathsf{P}\left(T > t_0 + (k+1)\Delta, T > t_0 + k\Delta\right) \\
=&\mathsf{P}\left(T > t_0 + k\Delta\right) - \mathsf{P}\left(T \leq t_0 + (k+1)\Delta, T > t_0 + k\Delta\right) \\
=&\mathsf{P}\left(T > t_0 + k\Delta\right) - \mathsf{E}\left\{\mathsf{E}\left\{1_{\{T \leq t_0 + (k+1)\Delta\}} \cdot 1_{\{T > t_0 + k\Delta\}} \middle| \mathcal{F}_{t_0 + k\Delta}\right\}\right\} \\
\overset{(a)}{=}&\mathsf{P}\left(T > t_0 + k\Delta\right) - \mathsf{E}\left\{1_{\{T > t_0 + k\Delta\}} \mathsf{E}\left\{1_{\{T \leq t_0 + (k+1)\Delta\}} \middle| \mathcal{F}_{t_0 + k\Delta}\right\}\right\} \\
=&\mathsf{P}\left(T > t_0 + k\Delta\right) - \mathsf{E}\left\{1_{\{T > t_0 + k\Delta\}} \mathsf{P}\left(T \leq t_0 + k\Delta + \Delta \mid \mathcal{F}_{t_0 + k\Delta}\right)\right\} \\
\overset{(b)}{<}&\mathsf{P}\left(T > t_0 + k\Delta\right) - \epsilon \mathsf{P}\left(T > t_0 + k\Delta\right) \\
\overset{(c)}{\leq}&(1-\epsilon)^{k+1},
\end{aligned} \quad (63)$$

where (a) is due to $\{T > t_0 + k\Delta\} \in \mathcal{F}_{t_0 + k\Delta}$, (b) is by (61) for $t = t_0 + k\Delta$, and (c) is by our assumption that (62) holds for k. Induction gives the desired result. It follows that

$$\begin{aligned}
\mathsf{E}\{T\} &= \int_0^\infty \mathsf{P}(T > \tau)\,\mathrm{d}\tau \\
&= \int_0^{t_0} \mathsf{P}(T > \tau)\,\mathrm{d}\tau + \sum_{k=0}^{\infty} \int_{t_0+k\Delta}^{t_0+(k+1)\Delta} \mathsf{P}(T > \tau)\,\mathrm{d}\tau \\
&\overset{(a)}{\leq} t_0 + \sum_{k=0}^{\infty} \mathsf{P}(T > t_0 + k\Delta) \cdot \Delta \\
&\overset{(b)}{\leq} t_0 + \Delta \sum_{k=0}^{\infty} (1-\epsilon)^k \\
&= t_0 + \frac{\Delta}{\epsilon} < \infty,
\end{aligned} \tag{64}$$

where (a) is by the fact that $\mathsf{P}(T > \tau)$ is a non-increasing function of τ and $\mathsf{P}(T > \tau) = 1$ for all $\tau \leq t_0$, and (b) is from (62). It completes the proof of Theorem 3. □

Acknowledgement

The author would like to thank Xiang Gao, Dr. Sichao Yang and Dr. Chong Li for their helpful discussions during the draft of this paper.

References

[1] Satosh Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009. `http://www.bitcoin.org/bitcoin.pdf`.

[2] Vitalik Buterin. Ethereum whitepaper. `https://github.com/ethereum/wiki/wiki/White-Paper`.

[3] Yoad Lewenberg, Yonatan Sompolinsky, and Aviv Zohar. Inclusive block chain protocols. In *Financial Cryptography*, 2015.

[4] Yonatan Sompolinsky, Yoad Lewenberg, and Aviv Zohar. Spectre: A fast and scalable cryptocurrency protocol, 2016. `https://eprint.iacr.org/2016/1159`.

[5] Yonatan Sompolinsky and Aviv Zohar. Phantom: A scalable blockdag protocol, 2018. `https://eprint.iacr.org/2018/104`.

[6] Serguei Popov. The tangle. `https://iota.org/IOTA_Whitepaper.pdf`.

[7] Anton Churyumov. Byteball: A decentralized system for storage and transfer of value. `https://byteball.org/Byteball.pdf`.

[8] Michael J. Fischer, Nancy A. Lynch, and Michael S. Paterson. Impossibility of distributed consensus with one faulty process. *J. ACM*, 32(2):374–382, April 1985.

[9] Cynthia Dwork, Nancy Lynch, and Larry Stockmeyer. Consensus in the presence of partial synchrony. *J. ACM*, 35(2):288–323, April 1988.

[10] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, OSDI '99, pages 173–186, Berkeley, CA, USA, 1999.

[11] Ethan Buchman. Tendermint: Byzantine fault tolerance in the age of blockchains. Master's thesis, The University of Guelph, Canada, 2016.

[12] David Williams. *Probability with Martingales.* Cambridge University Press, 1991.