Active Defense Analysis of Blockchain Forking through the Spatial-Temporal Lens

Shengling Wang, Senior Member, IEEE, Ying Wang, Hongwei Shi, and Qin Hu

Abstract—Forking breaches the security and performance of blockchain as it is symptomatic of distributed consensus, spurring wide interest in analyzing and resolving it. The state-of-the-art works can be categorized into two kinds: experiment-based and model-based. However, the former falls short in exclusiveness since the derived observations are scenario-specific. Hence, it is problematic to abstractly reveal the crystal-clear forking laws. Besides, the models established in the latter are spatiality-free, which totally overlook the fact that forking is essentially an undesirable result under a given topology. Moreover, few of the ongoing studies have yielded to the active defense mechanisms but only recognized forking passively, which impedes forking prevention and cannot deter it at the source. In this paper, we fill the gap by carrying out the active defense analysis of blockchain forking from the spatial-temporal dimension. Our work is featured by the following two traits: 1) dual dimensions. We consider the spatiality of blockchain overlay network besides temporal characteristics, based on which, a spatial-temporal model for information propagation in blockchain is proposed; 2) active defense. We hint that shrinking the long-range link factor, which indicates the remote connection ability of a link, can cut down forking completely fundamentally. To the best of our knowledge, we are the first to inspect forking from the spatial-temporal dimension. Our work is featured by the following two traits: 1) dual dimensions. We consider the spatiality of blockchain overlay network besides temporal characteristics, based on which, a spatial-temporal model for information propagation in blockchain is proposed; 2) active defense. We hint that shrinking the long-range link factor, which indicates the remote connection ability of a link, can cut down forking completely fundamentally. To the best of our knowledge, we are the first to inspect forking from the spatial-temporal perspective, so as to present countermeasures proactively. Solid theoretical derivations and extensive simulations are conducted to justify the validity and effectiveness of our analysis.

Index Terms—Blockchain, forking, spatial-temporal dimension, active defense.

I. INTRODUCTION

Blockchain has been burgeoning in a plethora of domains since its inception [1]–[4], due to the prominent traits of decentralization, transparency, traceability and immutability. Essentially, blockchain is a linear chain documenting valid transactions in a form of blocks, with each being approved by the distributed participants through consensus. The consensus mechanism functions nontrivially in preserving blockchain security since it guarantees that all the honest participants (or nodes) curate the unique shared chain, or denoted as the main chain, so as to maintain data consistency. However, there may arise disagreements among nodes over which the main chain is, and when this happens, we call the blockchain is forking.

Technically, forking refers to the phenomenon that there are a set of blocks \( B_h \) at the same height \( h \) at a time, i.e., \( |B_h| > 1 \) [5], as shown in Fig. 1. This suggests divergent blockchains are maintained among nodes, leading decentralized consensus to fail. Forking can be unintentional or intentional depending on the motivations behind. By “unintentional”, we mean forking is aroused due to the inefficient propagation of the overlay network without any adversary, while the “intentional” forking involves malicious attackers who aim at inserting new features for security breaches. It is, therefore, crucial to analyze forking since it destroys the distributed trust, threatening the security and performance of blockchain.

The state-of-the-art works on forking can be classified into two kinds, namely the experiment-based [6]–[8] and the model-based [9]–[12]. As the names suggest, the former studies clarify and evaluate the insights via experimental simulations while those of the latter are through mathematical deductions. However, the experiment-based analyses are exclusive, which means the observations drawn from one study may not be feasible for another since they are scenario-specific. This makes the experiment-based analysis an ill-posed problem in extracting decisive forking laws from the top level, falling short in guiding countermeasures effectively.

To remedy the deficiency of the experiment-based studies, the model-based analyses heaved in sight. However, most of them are constrained to the representation of time dimension, without considering the spatial characteristics of blockchain topology. Nonetheless, forking is essentially an undesirable result of main chain propagation dynamics, which is inevitably bound to the exact positions and connectivities of nodes located in the network. Consequently, such spatiality-free forking models are incompetent to figure out the fundamental problems.
mechanism of forking. Moreover, few studies have yielded to the \textit{active defense} mechanisms for thwarting forking but only recognized it passively, which caps forking prevention and cannot deter it from the root, thus motivating our work.

We face the \textit{heterogeneity-in-design} challenge in realizing an active defense analysis of blockchain forking through the spatial-temporal lens. That is, a fine-grained quantitative analysis with spatiality requires us to \textit{embed the connection heterogeneity into the main chain propagation mechanism.}

To resolve this, we endow “expansivity” for connections by differentiating them as the \textit{short-range link} and the \textit{long-range link}. Specifically, short-range links exist among direct neighbors while the long-range link can connect remote nodes probabilistically. As such, the short-range links have no expansivity since they can only spread information among geographically adjacent nodes, while the long-range links can transmit over a long distance with various probabilities, so that we claim they have greater expansivity. Accordingly, it is the differences in expansivity that mirror the connection heterogeneity. In addition, we take advantage of the two-dimensional grid network in \cite{15} to abstractly model the blockchain overlay network since recent theoretical developments have stated blockchain as a \textit{small-world phenomenon} \cite{14}-\cite{16}. In doing so, we come up with the definition of \textit{layer propagation} conceptually which characterizes the spread of information as the \textit{ripple effect}.

Despite the benefits, the introduction of short-/long-range links increases the complexity of spatial-temporal coupling analysis, which is referred to the second challenge in our paper. Detailedly, the remote transfer ability of the long-range links may accelerate main chain propagation with great uncertainty, complicating the propagation dynamics as a consequence. To deal with this, we thoroughly inspect the probability distributions of main chain propagation triggered by short-range links and long-range links respectively and propose two concepts, i.e., the \textit{activation time} and \textit{activation degree}, for modeling purposes, where the former denotes the time when the nodes of each layer first receive the main chain while the latter indicates the number of nodes that have received the main chain at any time. These two terms provide a direct clue for further depicting unintentional forking probability and intentional forking robust level, laying foundations for presenting an active defense mechanism to fight against forking.

To conclude, the main contributions of our paper can be summarized as follows:

- \textbf{Spatial-temporal propagation model of the main chain.} To begin with, we propose the first spatial-temporal model for the main chain propagation, by specifying the blockchain network as a two-dimensional grid with short-/long-range links. In light of this, the forking probability and robust level in unintentional and intentional scenarios are proposed, where the former is analyzed in various time scales, facilitating countermeasures with different intensities.

- \textbf{Active defense mechanism proposal.} Our work concludes that dwindling the \textit{long-range link factor} to change the connectivity of blockchain topology serves to cut down forking completely from the root. To the best of our knowledge, our work proposes the first active defense mechanism operatively to resist forking instead of following current recognitions passively.

- \textbf{Rigorous verifications.} Solid theoretical analyses and extensive simulations are conducted, which justify the validity of our forking models as well as the effectiveness of our active defense mechanism.

The rest of the paper is organized as follows. We first review the related work in Section \textbf{II} and characterize the network topology of blockchain with defined expansivity of links in Section \textbf{III}. Based on this, the activation time and activation degree are proposed in Sections \textbf{IV} and \textbf{V}. The modelings and analyses on the unintentional forking probability and intentional forking robust level are carried out in Sections \textbf{VI} and \textbf{VII}. Our experimental results are shown in Section \textbf{VIII} and Section \textbf{IX} finally concludes our paper.

\section{Related work}

At present, the growing interest in analyzing blockchain forking has produced a number of prominent investigations, which can be classified into two categories, i.e., the experiment-based and the model-based.

For the experiment-based forking analyses, Chen \textit{et al.} \cite{6} proposed a mechanism called GVScheme, which introduces the role of guarantor to effectively reduce the block verification time. And the simulation results manifest the efficacy of its mechanism in reducing the forking rate. Besides, a proximity-aware extension named Bitcoin Clustering Based Ping Time protocol (BCBPT) was presented by Fadihil \textit{et al.} in \cite{7}, which alleviates the forking phenomenon via improving the transactions propagation process. BCBPT was designed to realize this through evaluating the ping latencies between nodes, which has been testified to be strongly effective in optimizing the performance through extensive simulations. In \cite{8}, Zhang \textit{et al.} offered a backward-compatible defense mechanism to deal with selfish mining attack, allowing forking to be solved as a side problem. Through evaluating the proposed methods extensively, they concluded that the honest miners need to adopt the longest chain if it is at least 3 blocks ahead of the competitors so as to fight back attackers.

Parallel to the above efforts, the model-based analysis heaved in sight by Decker \textit{et al.} in \cite{9}, which quantitatively investigated the impact of information propagation on Bitcoin security from the macro level. To that aim, they proposed a probabilistic model to estimate the average forking rate based on the measurements of block spread across the network, and concluded that propagation delay causes forks primarily. Besides, Xiao \textit{et al.} in \cite{9} presented an analytical model to evaluate the effect of network connectivity on consensus security where various adversaries are involved. As such, both the forking rate and the revenue of miners are established to elucidate the security properties of consensus. To take precautions against forking, Wang \textit{et al.} \cite{11} studied the vulnerability of blockchain incurred by intentional forks through a delicate mathematical model, taking advantage of the large deviation theory. In their model, the number of created blocks from
the honest nodes and adversaries are regarded as dynamically growing queues, in which the difference between them can be analyzed to reflect the vulnerability of blockchain. Different from current efforts, Chen et al. in [12] explored the impact of competition among mining pools on forking from the miners’ perspective, based on which, a detailed model along with the derived closed-form formula of forking probability and expected mining revenue of each pool was expressed. Moreover, an evolutionary game framework was then developed to further reveal the long-term trends in the computing power distributions over pools.

However, the above two kinds of studies fall short in the following detriments. On the one hand, the experiment-based analyses are limited to specific scenarios, making the conclusions drawn from a certain case may be unreliable in another. As a result, they can not support forking prevention from the top level since universal and decisive forking laws are inaccessible. On the other hand, existing model-based researches suffer from spatiality-free which means they are restricted to the representation of time dimension while ignoring the spatial characteristics of blockchain topology. However, forking is highly related to spatiality in the sense that the propagation of forking is highly spatially dependent. Hence in this paper, the ongoing research only recognizes forking passively without proposing any active defense mechanism. Additionally, the derived closed-form formula of forking probability and long-term trends in the computing power distributions over pools.

As a result, they can not support forking prevention from the top level since universal and decisive forking laws are inaccessible. On the other hand, existing model-based researches suffer from spatiality-free which means they are restricted to the representation of time dimension while ignoring the spatial characteristics of blockchain topology. However, forking is highly related to spatiality in the sense that the propagation of forking is highly spatially dependent. Hence in this paper, the ongoing research only recognizes forking passively without proposing any active defense mechanism. Additionally, the derived closed-form formula of forking probability and long-term trends in the computing power distributions over pools.

### III. System model

#### A. Network topology

We exploit the two-dimensional grid network [13] to abstractly establish the underlying network of blockchain, as a response to the pioneer theoretical developments which abstractly establish the underlying network of blockchain. A small-world phenomenon [14]–[16] is highly related to spatiality in the sense that the propagation of forking is highly spatially dependent. Hence in this paper, the ongoing research only recognizes forking passively without proposing any active defense mechanism. Additionally, the derived closed-form formula of forking probability and long-term trends in the computing power distributions over pools.

**Definition 3.1 (Layer):**

- **Layer #0:** The set of nodes \( V_0 \) belongs to layer \#0 if the lattice distance between node in \( V_0 \) with \( s \) equals 1.
- **Layer \#j, j \in N^+:** The set of nodes \( V_j \) belongs to layer \#j if the lattice distance between node in \( V_j \) with \( s \) is \( (2^{j-1}, 2^j) \).

Assume the longest lattice distance between any node with \( s \) is \( n_{\text{max}} \geq 2 \), then we have \( 1 \leq j \leq \log n_{\text{max}}, j \in N^+ \). As shown in Fig. [3] nodes with lattice distance (1, 2) from node \( s \) compose layer \#1 (i.e., the green points), nodes with distance (2, 4) belong to layer \#2 (i.e., the yellow points), the same applies to other layers. If the farthest node receiving current main chain is \( u \), and the lattice distance between \( s \) and \( u \) meets \( 2^{j-1} < d(s, u) \leq 2^j \), then we state that \( u \in V_j \) and the main chain has been transmitted to layer \#j.

![Fig. 2: The topology of blockchain as a 9 \times 9 lattice for instance. To illustrate, nodes a and b are represented as (4, 3) and (7, 6) and the distance between them is 6. Note that the blue links are short-range links since the lattice distances between a and its neighbors are 1, and the red link is the long-range one since \( d(a, b) = 6 > 1 \).](image-url)

We claim that each node has four short-range links with neighbors determinately but has long-range links with some nodes probabilistically. In practice, the longer the spatial distance between two nodes, the less probability they have to possess a long-range link. Hence, we describe the probability that nodes \( v_1 \) and \( v_2 \) existing a long-range link, i.e., \( P_{\text{long}}(v_1, v_2) \), retains a negative exponential relationship with distance. That is, \( P_{\text{long}}(v_1, v_2) = d(v_1, v_2)^{-\beta} \) where \( \beta \) is the long-range factor to ensure \( d(v_1, v_2)^{-\beta} \in [0, 1] \). Remarkably, such a designed factor envisions a quantifiable mechanism to defense forking actively, which will be illustrated in Sections VI and VII.

#### B. Layer propagation

Once mining a new block, the creator will propagate it to all linked nodes, which then verify its validity and further transmit it to other connected nodes. Such a process continues until all the nodes accept this block, orchestrating the main chain propagation just like the ripple effect. Suppose the creator is node \( s \), we then introduce the concept of layer to capture the spread-out characteristics of information propagation in blockchain by presenting the following definition.
Recall the long-range link\(^1\) probability is defined as \( P_{\text{long}}(u,v) = d(u,v)^{-\beta} \) with the long-range factor \( \beta \). One may conclude that a smaller \( \beta \) induces a higher probability that the node can connect further, which in turn entitles a stronger potential to stretch more peripherally. That is to say, the long-range links also mirror various long-distance transmission capabilities, which brings in the following definition of expansivity.

**Definition 3.2 (Expansivity):** The expansivity \( \epsilon_L \) of link \( L \in \mathcal{E} \) with ends \( u,v \in \mathcal{V} \) is defined as \( \epsilon_L = P_{\text{long}}(u,v) \times \rho \) where \( \rho \) denotes the index of the layer where \( v \) locates if \( u \) is regarded as the creator.

According to Definition 3.2, the expansivity of a short-range link equals 0 since \( v \) belongs to layer \#0 in this case. As for a long-range link, its expansivity varies on the difference between \( \beta \) and the lattice distance. Notably, the difference in expansivity indeed reflects connection heterogeneity.

Now we are in the position to highlight the advantages of the short-/long-range links to manifest the merits of our system model. To begin with, the short-range links exist between neighbors certain, thus they offer great feasibility for intra-layer main chain propagation. On the contrary, the long-range link can probabilistically connect nodes when the lattice distance is larger than 1, which is often the case for nodes in different layers. Hence, the long-range links stand for the main pillar for inter-layer main chain propagation. To conclude, the short-/long-range links can cover various transmission cases of blockchain comprehensively. Additionally, the short-/long-range links with various expansivities are valuable for shaping the heterogeneity of links in blockchain. And it is the remote transfer ability of long-range links that breaks the regular pattern to propagate the main chain layer by layer, enabling cross-layer transmission. This facilitates a more pragmatic and realistic blockchain.

However, the combination of short-/long-range links challenges the rigorous inspection of main chain propagation. This is because the cross-layer transmission enabled by long-range links may accelerate information propagation with great uncertainty for inter-layer cases, perplexing the transmission dynamics. To remedy this, we first quantify the time when each layer \#\( j \) is first noticed by the main chain, i.e., the activation time \( \mathbb{E}[T(j)] \). Based on this, we can derive the activation degree \( I(t) \), defined as the number of nodes for each layer that has perceived the main chain at time \( t \), which finally realizes our main chain propagation model.

**IV. Activation Time**

In this section, we model the activation time of each layer to describe the absolute time when the nodes in each layer first accept the main chain. To achieve this, we carry out a relative-to-absolute method, which starts by introducing the adjacent propagation time to denote the relative time difference of layer \#\( j \) getting the main chain from layer \#\( j-1 \). After that, we deduce the corresponding absolute time by summing all the cases.

**Definition 4.1 (Adjacent propagation time):** The adjacent propagation time (APT) \( T_j \) refers to the arriving time that the main chain reaches layer \#\( j \), if the time of layer \#\( j-1 \) receives the main chain is set as 0.

Accordingly, APT denotes the interval of main chain propagation from layer \#\( j-1 \) to \#\( j \). Suppose the average transmission delays via short-/long-range links are denoted as \( \Delta_s, \Delta_l \), where \( \Delta_l \geq \Delta_s \) holds obviously. Then we can demonstrate APT for each layer in the following theorem.

**Theorem 4.1:** The expected adjacent propagation time of each layer \#\( j \geq 0 \), i.e., \( \mathbb{E}[T_j] \), can be summarized as

\[
\begin{align*}
\mathbb{E}[T_j] &= \Delta_s, & j = 0, 1, \\
\mathbb{E}[T_j] &> \tau^s_j (1 - (3 \times 2^{j-1})^{-\beta}) f_j \quad \text{(1)} \\
&> c \Delta_s \cdot 2^{j-2} (1 - (3 \times 2^{j-1})^{-\beta}) f_j, & j > 1,
\end{align*}
\]

where \( \tau^s_j \) denotes the time that layer \#\( j \) gets the main chain from \#\( j-1 \) via the long-range links, and \( f_j = N_{j-1} N_j \) with \( N_{j-1} \) and \( N_j \) being the number of nodes in \( \mathcal{V}_{j-1} \) and \( \mathcal{V}_j \).

**Proof:** When \( j = 0 \), the lattice distance between nodes in \( \mathcal{V}_0 \) to node \( s \) is 1, hence the propagation interval from \( s \) to \( \mathcal{V}_0 \) is \( \Delta_s \) via the short-range link; when \( j = 1 \), the lattice distance between nodes in \( \mathcal{V}_1 \) to node \( s \) is 2, indicating that of between nodes in \( \mathcal{V}_1 \) to nodes in \( \mathcal{V}_0 \) is 1. Hence the propagation interval from \( \mathcal{V}_0 \) to \( \mathcal{V}_1 \) is \( \Delta_s \) via direct short-range link due to \( \Delta_s \leq \Delta_l \). This justifies the first line of (1).

Since the short-/long-range links exist between nodes when their lattice distance is 1 or in adjacent layers, the main chain can be transmitted to layer \#\( j \) from \#\( j-1 \) via both of them. Hence, the APT of layer \#\( j \geq 1 \) can be characterized as

\[
\mathbb{E}[T_j] = P^l_j \cdot \tau^l_j + P^s_j \cdot \tau^s_j, \quad \text{(2)}
\]

where \( P^l_j \) and \( \tau^l_j \) denote the probability and time that layer \#\( j \) gets the main chain from \#\( j-1 \) via the long-range links, and \( P^s_j \) and \( \tau^s_j \) express those of via the short-range links. We name \( P^l_j \cdot \tau^l_j \) and \( P^s_j \cdot \tau^s_j \) respectively as the long-range and short-range parts which will be demonstrated more detailedly in the following.

(a) The long-range part. Denote the probability of nodes \( u \) and \( v \) residing in layer \#\( j-1 \) and \#\( j \) having the long-range link as \( p_{uv} \), then we have \( p_{uv} = d(u,v)^{-\beta} > (3 \times 2^{j-1})^{-\beta} \) because...
of \( d(u,v) < 2^{j-1} + 2^j = 3 \times 2^{j-1} \). Hence, the probability that node \( u \) does not possess long-range links with any node in layer \( \#j \) can be specified as \( \bar{p}_{u \rightarrow \#j} = \prod_{u \in V_j} (1 - p_{uv}) \). Let the number of nodes in \( V_j \) be \( |V_j| = N_j \), then we can obtain \( N_j = \sum_{i=2^{j-1}+1}^{2^j} 4i = 3 \times 2^{2j-1} + 2^j \) since there are \( 4i \) nodes whose lattice distance from node \( u \) is \( i \). In light of this, we can get

\[
\bar{p}_{u \rightarrow \#j} = \prod_{u \in V_j} (1 - p_{uv}) < \prod_{n_i=1}^{N_j} (1 - (3 \times 2^{j-1})^{-\beta}) = (1 - (3 \times 2^{j-1})^{-\beta})^{N_j}.
\]

(3)

Accordingly, the probability that any node in layer \( \#j-1 \) can not connect any node in layer \( \#j \) with long-range link can be formalized as \( \bar{p}_{\#j-1 \rightarrow \#j} = \prod_{u \in V_{j-1}} \bar{p}_{u \rightarrow \#j} = \prod_{u \in V_{j-1}} \prod_{v \in V_j} (1 - p_{uv}) \). Based on \( N_{j-1} = 3 \times 2^{2j-3} + 2^j \) and suppose \( f_j = N_{j-1}N_j = 9 \times 2^{2j-4} + 9 \times 2^{2j-3} + 2^j \), we can conclude that

\[
\bar{p}_{\#j-1 \rightarrow \#j} < (1 - (3 \times 2^{j-1})^{-\beta})^{f_j}.
\]

(4)

Hence, the probability that any node in layer \( \#j-1 \) has a long-range link with any node in layer \( \#j \) can be denoted as \( p_{\#j-1 \rightarrow \#j} = 1 - \bar{p}_{\#j-1 \rightarrow \#j} > 1 - (1 - (3 \times 2^{j-1})^{-\beta})^{f_j} \), which indicates that \( P_{ij} > 1 - (1 - (3 \times 2^{j-1})^{-\beta})^{f_j} \).

Notably, layer \( \#j \) receives the main chain from layer \( \#j-1 \) via the long-range link implies that during network transmission in layer \( \#j-1 \), there is a specific node (denoted as \( u^* \)) that has accepted the main chain, and also possesses a long-range link with nodes in layer \( \#j \) exactly. As a result, node \( u^* \) propagates the main chain to the next layer via this valuable long-range link. Let the first node accepting the main chain in layer \( \#j \) be \( u \). If \( u = u^* \), then \( \tau_{ij} = \Delta_i \). Otherwise, \( \tau_{ij} = d(u^*, u)\Delta_s + \Delta_l \) since node \( u \) needs to receive the main chain from node \( u^* \) through the short-range links internally. In this paper, we simply utilize the term \( \tau_{ij} \) for demonstration and leave an exact analysis of \( \tau_{ij} \) for future work. Until now, we can deduct the APT of layer \( \#j \) via the long-range link as

\[
E[T_{ij}^L] = P_{ij} \cdot \tau_{ij} > \tau_{ij} (1 - (1 - (3 \times 2^{j-1})^{-\beta})^{f_j}).
\]

(5)

(b) The short-range part. Since the short-range links only possess in neighbors whose lattice distance is 1, when the nodes in layer \( \#j \) propagate the main chain to the next layer through the short-range links, the distance to be passed will be no more than \( 2^{j-1} + 2^{j-2} = 2^{j-2} \). Hence, we can set \( E[\tau_{ij}^S] = c \cdot \Delta_s 2^{j-2} \) with \( c \) as the discounting factor to get the expectation. With this in mind, we can get the APT of layer \( \#j \) via the short-range link as

\[
E[T_{ij}^S] = P_{ij}^S \cdot \tau_{ij}^S = c \cdot \Delta_s 2^{j-2} (1 - P_{ij}^S).
\]

(6)

In summary, we can get the APT of layer \( \#j \) as shown in the second line of \([\text{I}]\) through combining the above two parts. This completes our proof.

It is worth noting that the defined APT only focuses on the propagation time of the main chain between nearby layers. To derive the whole expected propagation time of the main chain from the source node \( s \) to layer \( \#j \), i.e., \( E[T(j)] \), it is necessary to sum all the corresponding cases as presented in the following:

\[
E[T(j)] = \begin{cases} 
\Delta_s, & j = 0, \\
2\Delta_s, & j = 1, \\
2\Delta_s + \frac{j}{2} E[T_j], & j > 1.
\end{cases}
\]

(7)

Through substituting \([\text{I}]\) into (7), the expected activation time when the nodes in each layer \( \#j \) receive the main chain firstly can be summarized as

\[
E[T(j)] = \begin{cases} 
\Delta_s, & j = 0, \\
2\Delta_s, & j = 1, \\
2\Delta_s + \sum_{j=2}^{\infty} \frac{j}{2} E[T_j], & j > 1.
\end{cases}
\]

(8)

in which \( E[T(j)] > 2\Delta_s + \sum_{j=2}^{\infty} \frac{j}{2} [\Delta_s (1 - (3 \times 2^{j-1})^{-\beta})^{f_j} + c\Delta_s \cdot 2^{-j-2} (1 - (3 \times 2^{j-1})^{-\beta})^{f_j}] \).

V. Activation Degree

This section will illustrate the main chain propagation model by specifying the number of nodes that have received the main chain at any time, which is also denoted as the activation degree, based on the above analyses on activation time. To this end, we take advantage of the epidemic model, i.e., the susceptible-infected (SI) model \([\text{L}]\), to characterize the evolution of nodes in blockchain. SI models are widely exerted in topologically related information diffusion phenomenons, both in social and technology networks \([11], [18]–[20]\). We believe it is the simplest method to capture the essence of information propagation in blockchain. Technically, nodes have two states: susceptible (\( S \)) and infected (\( I \)), which are interchangeable. A node in state \( S \) indicates it is inactivated that has not received the main chain while that in state \( I \) means it has been activated by accepting the main chain. A node in \( S \) may turn into \( I \) once it accepts the main chain and work on it. In the following, we first derive the activation degree within layer locally, after which, we can obtain the global degree in the network scale.

We set the beginning of main chain diffusion in layer \( \#j \) \( > 1 \) as time \( T = 0 \), and the activation and inactivation degrees (or the number of nodes that are in state \( I \) or \( S \)) are denoted as \( I_j(\omega) \) and \( S_j(\omega) \) respectively in any time \( T = \omega > 0 \). Then we have \( I_j(\omega) + S_j(\omega) = N_j \) and \( I_j(0) = 1 \) since there must be one activated node initially. Based on the SI model, \( I_j(\omega) \) can be derived as:

\[
\begin{cases} 
\frac{dI_j(\omega)}{d\omega} = \alpha_j I_j(\omega)(N_j - I_j(\omega)), \\
I_j(0) = 1,
\end{cases}
\]

(9)

where \( \alpha_j \) represents the probability that an activated node transfers the main chain to others within layer \( \#j \). Considering nodes inside the layer transfer information via short-range links, \( \alpha_j \) can also be interpreted as the probability that a node possesses the short-range link with others, which is \( \alpha_j = \frac{4}{N_j-1} \). In doing so, we can derive \( I_j(\omega) \) formally through the logistic model, leading to

\[
I_j(\omega) = \frac{N_j}{1 + (N_j - 1)e^{-\alpha_j N_j \omega}}.
\]

(10)
Notably, $I_j(\omega)$ in (10) depicts the number of activated nodes in time $\omega$ of layer $#j$ locally. Subsequently, we are going to find the activation degree globally, i.e., $I(t)$, which expresses the number of infected nodes in the network at $T = t$ from the very beginning when the source node produces the main chain. We reset $T = 0$ as the time when the main chain is originally generated, in light of the above analysis, we can acquire the following theorem.

**Theorem 5.1:** The activation degree of the network $I(t)$ when $0 < t < T(J), J \in [0, \log n_{max}], J \in \mathbb{N}^+$, satisfies

$$I(t) = \begin{cases} 
1, & 0 < t < T(0), \\
5, & T(0) \leq t < T(1), \\
13, & T(1) \leq t < T(2), \\
13 + \sum_{j=3}^{J-1} I_j(t - T(j)), & T(2) \leq t < T(J).
\end{cases}$$

(11)

**Proof:** We prove each case of (11) in the following.

1. Case 1: The activation degree of the network $I(t_0) = 1$ since layer $#0$ has not received the main chain when $t_0 \in (0, T(0))$ according to (7), shown as the blue node in Fig. 3.

2. Case 2: The activation degree of the network $I(t_1) = 5$ since layer $#0$ can receive the main chain when $t_1 \in [T(0), T(1))$, leading to the four directly connect neighbors being activated, shown as the blue and red nodes in Fig. 3.

3. Case 3: The activation degree of the network $I(t_2) = 17$ since both layer $#0$ and $#1$ can receive the main chain when $t_2 \in [T(1), T(2))$, making $I(t_2) = I(t_1) + N_1 = 13$, shown as the blue, red and green nodes in Fig. 3.

4. Case 4: when $t_3 \in [T(2), T(J)]$ s.t. $2 < j \leq J$, layers $#0 \sim #j - 1$ all have accepted the main chain. Take layer $#3$ as an example, the activation time of this layer is $T(3)$. Hence, the main chain has been propagated within this layer for $\Delta t = t_3 - T(3)$, making the activation degree in this layer as $I_3(\Delta t_3)$. Other layers can be done in the same manner, leading to the fact that $I(t_3) = I(t_2) + \sum_{j=3}^{J-1} I_j(\Delta t_j)$.

Until now, we present the activation degree at any time in the network, which can be recognized as the main chain propagation model. Such a measurement is so valuable in reflecting the possible forking occurrence since the higher the degree is, the more nodes perceive the main chain, the less probability that forking may happen. In the following two sections, we carry out forking analysis for both unintentional and intentional scenarios, based on which, an active defense mechanism can be proposed.

**VI. MODELING AND ANALYSIS: UNINTENTIONAL FORKING**

Technically, unintentional forking is normally caused by the inefficient propagation of the blockchain overlay network without any attacker or artificial manipulation [5], [21]. Trace the root, it happens when a conflict block $B$ is found while the previous block $A$ with the same height is propagated in the network. Accordingly, we claim that the unintentional forking probability is equivalent to that of generating new blocks (i.e., $B$) during the propagation of chain containing $A$.

Assume the source node starts to transmit the produced main chain at time $t = 0$, and all the nodes are supposed to accept the main chain at $\Delta t = T_{all}$ if no forking occurs. The whole time span of $T_{all}$ can be equally divided into $\frac{\Delta t}{\delta}$ intervals, with each interval being $\delta$. In the following, we proceed to analyze the probability of unintentional forking both in unit time, i.e., $f_r(t)$, and over a period of time, i.e., $F_R(t)$, where the former focuses on each interval $[t, t + \delta]$ while the latter specifies any defined period $[0, t + \delta]$ with $t \in [0, T_{all} - \delta]$. In doing so, effective countermeasures of unintentional forking are facilitated operatively at different time scales with multiple intensities.

### A. Unintentional forking probability analysis in unit time

In fact, the mainstream consensus mechanism, i.e., *proof-of-work* (PoW), guarantees that the average work of each node follows Bernoulli distribution, which suggests that the mining process can be deemed as a Poisson process [5], [11]. Let $\Omega(t)$ be the set of nodes which have not received the main chain at time $t$ and $\varphi(t)$ denotes the number of conflict blocks created by the nodes in $\Omega(t)$ at time $t$. Hence, $\varphi(t)$ follows Poisson distribution with expectation $\lambda = \sum_{u \in \Omega(t)} \pi_u$, with $\pi_u$ denoting the computing power of node $u$. As such, we can obtain the probability that $k$ new blocks are generated during $[t, t + \delta]$ as

$$P[\varphi(t + \delta) - \varphi(t) = k] = \frac{e^{-\lambda\delta} (\lambda\delta)^k}{k!}.$$  

(12)

Note that $k = 0$ elaborates there is no block created by the activated nodes in $\Omega(t)$, which in turn indicates no unintentional forking occurrence. Therefore, we can derive the probability of unintentional forking as $f_r(t) = 1 - P[\varphi(t + \delta) - \varphi(t) = 0] = 1 - e^{-\delta \sum_{u \in \Omega(t)} \pi_u}$. If the computing power is uniformly distributed among nodes, we have

$$f_r(t) = 1 - e^{-\delta |\Omega(t)| \pi_u} = 1 - e^{-\delta S(t) \pi_u},$$  

(13)

where $S(t) = N_{total} - I(t)$ with $N_{total} = \sum_{i=1}^{n} 4i + 1 + 2n + n^2$ and $I(t)$ is formalized in (11). Through investigating (13) thoroughly, we claim the following corollaries to reveal the inherent mechanism of unintentional forking in unit time, thus we can present direct evidence to hinder it operatively.

**Corollary 6.1:** A smaller long-range factor $\beta$ can induce a lower $f_r(t)$.

**Proof:** As described above, $\beta$ specifies the probability that any node pair $u$ and $v$ has a long-range link. The lower $\beta$ is, the more likely such link will exist. In addition, the long-range link facilitates the synchronicity of cross-layer main chain propagation, which allows more nodes to receive the main chain earlier, making the number of susceptible nodes smaller. Aware of this, we can clarify that a lower $\beta$ enables the main chain to be broadcasted to the whole network more efficiently through more long-range links, shrinking the unintentional forking probability as a consequence.

**Corollary 6.2:** The unintentional forking probability $f_r(t)$ goes down when the transmission delays of the short-long-range links, i.e., $\Delta_s$ and $\Delta_l$, decline.

**Proof:** As demonstrated in Theorem 4.1 and (8), a lower $\Delta_s/\Delta_l$ will decrease the expected APT as well as the activation time for each layer $#j$. This will in turn influence $I(t)$ in
positively while affect $S(t)$ negatively, indicating a lower forking probability as formalized in (13). An intuition for this is that lower transmission delays make blockchain consume less time to hear the main chain for the inactivated nodes. This leaves no room for them to produce competitive blocks at the same height, decreasing forking probability consequently.

B. Unintentional forking probability analysis over a period of time

In this section, we formalize the probability of unintentional forking during a period of time $[0, t + \delta]$, i.e., $FR(t)$. According to subsection VI-A, the forking probability in $[t, t + \delta]$ is denoted as $fr(t)$, then $FR(t)$ turns to

$$FR(t) = 1 - \prod_{w=0}^{t} (1 - fr(w)) = 1 - \prod_{w=0}^{t} e^{-\delta \sum_{u \in \Omega(w)} \pi_u}$$  \hspace{1cm} (14)

When the computing power is allocated uniformly, $FR(t)$ becomes $1 - e^{-\delta \pi_u \sum_{w=0}^{t} S(w)}$. We then give the following corollaries.

**Corollary 6.3:** A smaller long-range factor $\beta$ can bring about a lower $FR(t)$.

**Corollary 6.4:** $FR(t)$ drops when $\Delta_s$ and $\Delta_l$ decrease.

The proofs of these two corollaries are similar to those of Corollaries 6.1 and 6.2, so we omit them for simplicity.

VII. Modeling and Analysis: Intentional Forking

Differently with unintentional forking, intentional forking involves malicious adversaries, who aim to surreptitiously execute the PoW for creating a chain containing fake transactions, namely the fake chain [11]. If the fake chain is longer than the honest main chain, the latter is then substituted by the malicious fake one according to the longest chain principle, incurring intentional forking attack as a consequence.

In particular, the adversaries always commence the forking attack assembly as a group since the honest majority makes it challenging for an attacker to commit attacks solely. In such an adversarial group, members share knowledge of the fake chain and information interchange is required to be real-time so as to prompt the success probability of attack. Considering this, we can assume there is no transmission delay among the group which can be realized through maintaining the participants in a local area network (LAN). Based on this, Wang et al. in [11] presented the robust level $\vartheta$ of blockchain being attacked by intentional forking through analyzing the computational confrontation between the honest and malicious nodes, that is

$$\vartheta = - \frac{\log \epsilon}{\log \frac{\Lambda}{\Lambda_e}}$$ \hspace{1cm} (15)

where $\epsilon \in [0, 1]$ is a preset threshold indicating the vulnerability probability of blockchain should be less than. In addition, $m$ and $e$ describe the number of nodes that have received the honest main chain and fake chain, $\gamma$ and $\Lambda$ represent the computing power of the honest and malicious node on the premise of uniform distribution. Essentially, $\vartheta$ suggests the required difference in the number of blocks completed by the adversary and the honest node, to verify a transaction. The higher $\vartheta$ is, the more effort should be put to launch attacks, the safer the blockchain being protected from intentional forking.

However, the above formulation falls short in static modeling and spatiality-free, making it insufficient in depicting a real-time and pragmatic blockchain. Aware of this, we present a dynamic robust level with spatiality, i.e., $\theta(t)$ as follows:

$$\theta(t) = - \frac{\log \epsilon}{\log \frac{\Lambda(t)}{\Lambda_e}}$$ \hspace{1cm} (16)

where $I(t)$ is determined as (11). This gives the following corollaries.

**Corollary 7.1:** A smaller long-range factor $\beta$ can lead to a higher $\theta(t)$, thus making blockchain stronger in fighting against intentional forking.

**Corollary 7.2:** $\theta(t)$ raises when $\Delta_s$ and $\Delta_l$ decrease, which indicates that dwindling the transmission delays can help to hinder intentional forking.

These two corollaries can be easily derived, therefore we omit their proofs for simplicity.

Remark. Here we are going to highlight the significant merits of all the proposed corollaries in facilitating an active defense mechanism for thwarting forking. Note that for both unintentional and intentional scenarios, setting a smaller $\beta$ and $\Delta_s/\Delta_l$ will lead to a lower forking probability and promote the robustness of blockchain, which means 1) increasing the long-range link between any two nodes and 2) dwindling the transmission delays of the short-/long- range links are the two effective countermeasures. This provides clear evidence for blockchain designers to devise and detect the topology and transmission capacity of the network so as to meet our requirements in fighting back forking. More excitingly, our paper proposes the first active forking defense mechanism, that is, positively reshaping the overlay network through decreasing the long-range factor $\beta$. In doing so, we can eradicate the forking phenomenon fundamentally.

VIII. Experiments

In this section, we will evaluate the validity and effectiveness of our proposed models and active defense mechanism. We have simulated the blockchain network with the PoW consensus mechanism written by Python, running on machines equipped with Intel Core i7-8700 GPU, 3.20 GHz CPU and 8 GB RAM. We begin by verifying our main chain propagation model in subsection VIII-A after that, the unintentional and intentional forking models established in Sections VI and VII are analyzed respectively in subsections VIII-B and VIII-C.

A. Evaluation on the main chain propagation model

We first carry out experiments on the activation degree $I(t)$ and compare it with the theoretical results, to demonstrate the validity of our proposed models. To calculate $I(t)$, we simulate the topology of blockchain as the aforementioned grid of $N_{total} = 145$ and 545 nodes with short-/long- range links. Besides, the probability of the long-range link between
any node pair \( u \) and \( v \) is preset as \( P_{\text{long}} = d(u, v)^{-\beta} \) where \( \beta = 1 \) and 10. The transmission delays are determined as \( \Delta_s = 1 \) and \( \Delta_l = 1 \) respectively. Note the tested system is driven by PoW consensus and we fix the interval \( \delta \) as \( \Delta_s \) for better performance. Each experiment is repeated 50 times to get the average result for statistic confidence.

Fig. 4 reports the theoretical and simulated results of \( I(t) \) on the difference of \( t \) when \( \beta = 1 \) and 10 and \( N_{\text{total}} = 145 \) and 545. Conclusively, we make the following observations: 1) our experimental and analytical results match perfectly under various network sizes and topologies. This demonstrates the validity of our main chain propagation model in depicting the information diffusion of blockchain. 2) From subfigures (a) and (c), we can conclude that under the same network size with \( N_{\text{total}} = 145 \), the increase of \( \beta \) will impose a negative effect on \( I(t) \). More specifically, when \( t = 6 \), the activation degree \( I(t) \) of \( \beta = 1 \) is nearly 120 in the simulation (or 110 theoretically), while that of \( \beta = 10 \) is 80 approximately in the simulation (or 70 theoretically). One conjecture is that a higher \( \beta \) may trigger a lower probability of possessing a long-range link between any nodes \( u \) and \( v \), slowing down the propagation process cross-layer and consequently declining the number of activated nodes. The same conclusion can also be acquired from subfigures (b) and (d). 3) From subfigures (a) and (b), we can find that when \( \beta \) is identical, the network with \( N_{\text{total}} = 145 \) realizes consensus globally earlier than that of with \( N_{\text{total}} = 545 \), which reports a smaller network is much easier to reach consistency. Detailedly, all the nodes get the main chain when \( t = 9 \) in the network with 145 nodes, while \( I(t) \) in the network with 545 nodes stops raising until \( t = 17 \). The same can be concluded from subfigures (c) and (d).

B. Evaluation on the unintentional forking model

After testifying the validity of the main chain propagation model \( I(t) \), we proceed to evaluate the performance of forking probabilities \( fr(t) \) and \( FR(t) \) in unintentional forking. Besides the above described experimental settings, we set the computing power of each node equally and bring in the transmission delay ratio \( \Delta \) in which \( \Delta = 1 \) means the initially set \( \Delta_s = 1 \) and \( \Delta_l = 1.5 \), and \( \Delta = 1.1 \) represents \( \Delta_s' = 1.1\Delta_s \) and \( \Delta_l' = 1.1\Delta_l \).

We plot the evolutions of unintentional forking probability in unit time \( fr(t) \) in Figs. 5 and 6. Specifically, Fig. 5 displays the negative relationship between \( fr(t) \) and \( t \), when \( \beta = 1 \) and 10 and \( N_{\text{total}} = 145 \) and 545. That is, the forking phenomenon can be hindered probabilistically if the main chain is spread
The forking probability over a period of time $FR(t)$ when $\beta = 1$ and 10.

Fig. 8: The forking probability over a period of time $FR(t)$ when $\Delta = 1$ and 1.1.

long enough. In addition, the fact that the orange lines lie above the blue ones shows that a lower $\beta$ will lead to a smaller forking probability, corroborating Corollary 6.1 as a result. Fig. 6 exhibits the effect of transmission delays on $fr(t)$, which varies with the propagation time $t$ on the difference of $\beta$ and $N_{total}$. The subfigures in Fig. 6 suggest that higher delays will trigger forking with a higher probability as we can inspect that the orange lines locate above the blue ones. This proves what we state in Corollary 6.2.

The trends of unintentional forking probability over a period of time, i.e., $FR(t)$, are presented in Figs. 7 and 8 based on which, we can find 1) $FR(t)$ grows as time goes by but with a gradually decreasing rate, which agrees with the proposed analytical model as shown in (14). Theoretically, $FR(t)$ is formalized according to the summation of $S(w)$, that is, the number of suscepable nodes from $w = 0$ to $w = t$, which increases with a declining growth rate as more and more nodes accept the main chain. 2) A smaller $\beta$ can incite a lower forking probability as we derived in Corollary 6.3 according to Fig. 7. 3) Fig. 8 testifies the effectiveness of Corollary 6.4 in that the forking probability over a period of time $FR(t)$ drops as the decrease of the transmission delays. To conclude, a blockchain overlay network with a lower long-range factor $\beta$, a smaller network size $N_{total}$ and less delays $\Delta s/\Delta l$ will endure the least risk of being attacked by unintentional forking.

C. Evaluation on the intentional forking model

In this section, we evaluate the dynamic robust level with spatiality, i.e., $\theta(t)$, for the intentional forking scenario. Assume there are $e = 20$ malicious nodes, where the threshold $\epsilon$ is preset as 0.1. The results are demonstrated in Figs. 9 and 10. Fig. 9 reports the relationship between $\theta(t)$ and $t$, from which we can conclude that as time goes by, the robust level will increase since the decrease of $\theta(t)$ denotes less block difference is required for hindering forking occurrence. Besides, it is testified that a smaller $\beta$ can lead to higher $\theta(t)$, as the blue lines are always below the orange ones. This justifies the validity of Corollary 7.1. Additionally, Fig. 10 shows $\theta(t)$ varies with $t$ when different $\Delta s$ and $\Delta l$ are adopted, where we can find lower delays can help promote the robust level as clarified in Corollary 7.2.

IX. Conclusion

In this paper, we carry out the first active defense analysis of blockchain forking from the spatial-temporal dimension. To begin with, we characterize the topology of blockchain network as a two-dimensional grid with distinguished short-/long-range links. Based on this, the concepts of layer and expansivity are defined to respectively capture the ripple-effect information propagation process and connection heterogeneity of blockchain. In addition, we propose the term of activation time to denote the time when the nodes in each layer first accept the main chain, in light of which, we finally realize the activation degree to express the main chain propagation
model. In doing so, the forking probability and robust level in unintentional and intentional forking are modeled and inspected detailedly. Through our analyses, we conclude that 1) dwindling the transmission delays of the short-/long- range links can hinder forking and 2) positively reshaping the overlay network through shrinking the long-range factor $\beta$ can resolve the forking phenomenon from the root. This observation is so valuable that it delivers the first forking defense mechanism proactively and operatively. Extensive theoretical deductions and simulations are conducted to verify the effectiveness of our analysis.

**ACKNOWLEDGMENT**

This work has been supported by National Key R&D Program of China (No. 2019YFB2102600), National Natural Science Foundation of China (No. 61772044), the International Joint Research Project of Faculty of Education, Beijing Normal University, and Engineering Research Center of Intelligent Technology and Educational Application, Ministry of Education.

**REFERENCES**

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *Decentralized Business Review*, p. 21260, 2008.

[2] V. Buterin et al., “A next-generation smart contract and decentralized application platform,” *white paper*, vol. 3, no. 37, pp. 2–1, 2014.

[3] Y. Wang, Z. Su, Q. Xu, R. Li, and T. H. Luan, “Lifesaving with reschain: Energy-efficient and partition-tolerant blockchain based secure information sharing for uav-aided disaster rescue,” in *IEEE INFOCOM 2021-IEEE Conference on Computer Communications*. IEEE, 2021, pp. 1–10.

[4] B. C. Ghosh, T. Bhartia, S. K. Addya, and S. Chakraborty, “Leveraging public-private blockchain interoperability for closed consortium interfacing,” in *IEEE INFOCOM 2021-IEEE Conference on Computer Communications*. IEEE, 2021, pp. 1–10.

[5] H. Shi, S. Wang, Q. Hu, and X. Cheng, “Micro analysis of natural forking in blockchain based on large deviation theory,” *arXiv preprint arXiv:2105.09535*, 2021.

[6] J. Chen and Y. Qin, “Reducing block propagation delay in blockchain networks via guarantee verification,” in *2021 IEEE 29th International Conference on Network Protocols (ICNP)*. IEEE, 2021, pp. 1–6.

[7] G. Owenson, M. Adda et al., “Proximity awareness approach to enhance propagation delay on the bitcoin peer-to-peer network,” in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2017, pp. 2411–2416.

[8] R. Zhang and B. Preneel, “Publish or perish: A backward-compatible defense against selfish mining in bitcoin,” in *Cryptographers Track at the RSA Conference*. Springer, 2017, pp. 277–292.

[9] C. Decker and R. Wattenhofer, “Information propagation in the bitcoin network,” in *IEEE P2P 2013 Proceedings*. IEEE, 2013, pp. 1–10.

[10] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, “Modeling the impact of network connectivity on consensus security of proof-of-work blockchain,” in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE, 2020, pp. 1648–1657.

[11] S. Wang, C. Wang, and Q. Hu, “Forking by forking: Vulnerability analysis of blockchain,” in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE, 2019, pp. 829–837.

[12] C. Chen, X. Chen, J. Yu, W. Wu, and D. Wu, “Impact of temporary fork on the evolution of mining pools in blockchain networks: An evolutionary game analysis,” *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 1, pp. 400–418, 2020.

[13] J. Kleinberg, “The small-world phenomenon: An algorithmic perspective,” in *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, 2000, pp. 163–170.

[14] T. Wang, C. Zhao, Q. Yang, S. Zhang, and S. C. Liew, “Ethn: Analyzing the underlying peer-to-peer network of ethereum blockchain,” *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2131–2146, 2021.

[15] B. Tao, I. W.-H. Ho, and H.-N. Dai, “Complex network analysis of the bitcoin blockchain network,” in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2021, pp. 1–5.

[16] D. D. F. Maesa, A. Marino, and L. Ricci, “Uncovering the bitcoin blockchain network,” in *2021 IEEE International Conference on Data Science and Advanced Analytics (DSAA)*. IEEE, 2021, pp. 1–6.

[17] T. Zhou, J.-G. Liu, W.-J. Bai, G. Chen, and B.-H. Wang, “Behaviors of susceptible-infected epidemics on scale-free networks with identical infectivity,” *arXiv preprint arXiv:2105.09535*, 2021.

[18] W. O. Kermack and A. G. McKendrick, “A contribution to the mathematical theory of epidemics,” *Proceedings of the royal society of london. Series A, Containing papers of a mathematical and physical character*, vol. 115, no. 772, pp. 700–721, 1927.

[19] J. Kleinberg, “The small-world phenomenon: An algorithmic perspective,” in *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, 2000, pp. 163–170.