IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Blockchain Architecture Reliability-Based Measurement for Circuit Unit Importance

Jie Xiao[1], Jungang Lou[2,4], Jianhui Jiang[3], Xiaoxin Li[1], Xuhua Yang[1], Yujiao Huang[1]*

[1] College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou, 310023 China
[2] College of Information Science, Huzhou University, Huzhou, 313000 China
[3] School of Software Engineering, Tongji University, Shanghai, 201804 China
[4] Department of Computer Science, the University of Texas at San Antonio, San Antonio, TX 78249 USA

*Corresponding author: Jungang Lou (e-mail: loujungang0210@hotmail.com).

This work was supported by the National Natural Science Foundation of China (No. 61502422, 61772199, 61772198, 61432017, 61503338 and 61773348), the Natural Science Foundation of Zhejiang Province (Nos. LY18F020028, LQ15F020006, LY18F020031, LY18F030023 and LY17F030016) and the Natural Science Foundation of Zhejiang University of Technology (No. 2014XY007).

ABSTRACT Currently, few works focus on the reliability of the blockchain architecture at the circuit level, which makes its security and privacy vulnerable to hardware errors. To mitigate the hazard, through an iterative probabilistic transfer matrix model coded by a binary-decimal mechanism, a reliability-based evaluation method for the importance of circuit units is proposed in this paper. First, the method calculates the output reliabilities in any leads by the iterative probabilistic transfer matrix model and obtains the reliability gradient for the circuit units based on the gradient and barrel theory. Second, it sorts the importance of the circuit units based on their obtained reliability gradients. Third, combining the sensitized path coverage rate and the sequence comparison, the method constructs an importance-based sorting algorithm for the circuit units with the same reliability gradients. Finally, it reinforces the importance circuit units based on the sorting results to improve the security and privacy for the blockchain architecture at the hardware level. Theoretical analysis and experimental results indicate that the proposed method can be applied to measure the importance of circuit units at several abstract levels, with high precision and small time-space complexity, and systems can thus achieve a great reliability improvement at a small cost.

INDEX TERMS blockchain architecture reliability, hardware-level, reliability gradient, circuit unit, importance measurement

I. INTRODUCTION

The blockchain is the core mechanism for Bitcoin [1], and its purpose is to solve the credit problems of both sides of the transaction in a decentralized environment, which can greatly improve transaction efficiency and reduce costs [2] since it allows payment to be finished without any banks or intermediaries. Additionally, a blockchain can be applied in other fields, including smart contracts, public services, reputation systems and security services. Therefore, it can be said that the blockchain will occupy an increasingly important position in people's daily lives, and its architecture reliability will directly affect people's property security [3]. Where, architecture reliability is defined as the fault-tolerant probability of the architecture.

Currently, research on the reliability of blockchain architectures is mainly focused on the software level [4]. For example, Ref. [5] proposed a novel integrated factor communication tree algorithm to improve the efficiency and reliability of blockchain communication. Ref. [6] demonstrated that an attacker's access to extra computational power could disrupt the honest mining operation in a blockchain cloud and provided some preventive measures. In fact, with the progress of technology, hardware attacks have developed into one of the most important types of hacking methods, which seriously threatens the reliability of blockchain architectures [7]. Therefore, it is necessary to strengthen the reliability of blockchain architectures at the hardware level to ensure the security and privacy of blockchains.

Currently, the mainstream of hardware development is intellectualization and miniaturization, which prompts us to improve the reliability of blockchain architectures at the circuit level so that they can achieve a great improvement at a small cost. However, when the device feature sizes sharply decrease, the manufacturing process becomes more complex, inevitably introducing more defects, which causes the circuit

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2800712, IEEE Access

reliability to face the threat of functional faults and the challenge of parametric faults [8, 9]; traditional methods with coarse-grained and highly reliable design cannot satisfy the chip miniaturization requirement [10]. Therefore, in recent years, increasing numbers of researchers in industrial and academic circles are attempting to find highly reliable circuit design methods with fine granularity to alleviate the current plight [11-13].

The key to designing highly reliable circuits based on fine-grained methods is to accurately position the reliability-sensitive circuit units, which requires accurately evaluating the reliability gradient of each circuit unit and can reflect the importance of each circuit unit based on reliability in the circuit structure. However, only a few circuit units tend to be considered in engineering practice. Because many factors must be balanced in that condition, the common practice is to select the circuit units with the largest effect on reliability to reinforce [10, 13]. To improve the reinforcement effect, it is necessary to study an importance measurement method to sort the important circuit units based on reliability, where the important circuit units have a large effect on the circuit reliability.

Currently, the methods used to measure reliability-based important circuit units are mainly concentrated in the field of reliability testing [14, 15]. In the early stages of circuit design, to measure the importance of circuit units, the common practice is as follows. First, insert a fault point into the netlist and set different fault probabilities. Second, analyze the changes of the circuit reliability for different inputs and identify the result as an important value for the circuit unit marked in the first step. However, this approach requires exponential time consumption to simulate circuit faults and input vectors and lacks the capacity for dynamic assessment, which makes it fail to measure the importance of circuit units in the design process. In addition, the method does not provide a more efficient quantization strategy for the circuit units with the same test results, which is not conducive to achieving the goal of a highly reliable circuit design based on a fine-grained strategy. In the chip-manufacturing stage, the common practice is as follows. First, use some additional hardware device, such as an active probe, metal clip or dedicated circuit board, to inject faults into the target chip by pins; second, collect the failure data to analyze the chip reliability under different stress conditions. The method can simulate actual hardware faults, but it normally requires an additional hardware device and fault injectors, which easily introduce new faults to the target chip and become difficult or even impossible to design for the current high-complexity, high-speed chips. Therefore, locating the important circuit units in the early stage of circuit design will help to identify the weaknesses of the hardware system in time so that they can be reinforced, which helps the blockchains run on reliable hardware.

However, three issues must be addressed to measure the importance of circuit units in the early stages of circuit design: (1) the time-space complexity, as excessive computational complexity will reduce the practicability of the method; (2) the dynamic measurement of the importance of circuit units, which is helpful for timely decision-making; and (3) the measurement accuracy, which is beneficial to correct decision-making. In response to these requests, we have found that the iterative probabilistic transfer matrix model with hybrid coding (EPTM) [16] can accurately evaluate the circuit reliability, that its time-space complexity increases linearly with the number of circuit units and that it can be used to calculate the output reliabilities in any leads. Therefore, the EPTM model is selected as a platform to study the importance measurement of circuit units. In addition, the analysis found that the circuit units with the same reliability gradient had identical effects in improving the weakness of circuits, but they had different effects on the reliabilities of the other circuit units because of the difference in sensitized path coverage. Therefore, the importance of the circuit units with the same reliability gradients must be further analyzed to improve the calculation precision. The sensitized path coverage rate of the circuit unit is the ratio between the number of circuit units covered by the accessible paths from the circuit unit to the primary outputs and the number of all circuit units.

In summary, to improve the reliability of blockchain architectures using the fine-grained strategy, this study will expand on the following steps. First, use the calculation properties of the EPTM model to extract the output reliabilities in any leads. Second, calculate the reliability gradient of the circuit units using gradient and barrel theories to satisfy the requirement of dynamic measurement. Third, construct an importance measurement method for the circuit units with the same reliability gradients using the information of their sensitized path coverage rate to further improve its accuracy. Fourth, sort the circuit units based on their importance using the sequence comparison. Finally, demonstrate the effectiveness of the proposed method using the Monte Carlo method.

This rest of the paper is organized as follows. Section 2 proposes an importance measurement method for circuit units. The experimental results on circuits are analyzed and discussed in Section 3. Section 4 presents the study's conclusions.

II. Importance Measurement Method for Circuit Units

To satisfy the requirement of dynamic measurement with high accuracy and low time-space complexity and to improve the reliability of blockchain architectures, we mainly conduct three works: first, a dynamic reliability evaluation method with high accuracy and low computational complexity; second, an effective quantification model for the importance of circuit units with high accuracy; and third, an effective algorithm that can dynamically measure the importance of circuit units.

A. EPTM model

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2800712, IEEE Access

The EPTM model realizes a blocking treatment to the concurrent signals in fan-out by hybrid coding, and it solves the problem of the excessive time-space complexity in the traditional PTM model [17] using an iterative calculation strategy. Its steps are expressed as follows. First, initialize the primary input signals and circuit units using the hybrid coding strategy. Second, construct the input vectors and input reliability matrixes for circuit units using a virtual method with a weak equivalence principle. Third, perform the matrix multiplication of the input reliability matrix by the probabilistic transfer matrix of the corresponding circuit unit. Finally, obtain the output reliability of the circuit unit by multiplying its input vector with the above-obtained result. The computational process is shown in Fig. 1. An illegal element is an element that consists of binary coding and decimal coding and includes the illegal code segment "11" in its binary coding; the binary codings of the elements perform the bitwise-or operation, and their decimal codings perform the multiplication operation; *PIS*s are the primary input signals; *g* is a circuit unit; *RPM* and *RIM* are the input reliability matrix and ideal input matrix of *g*, respectively; *PID* and *POD* are the input vector and output vector for *g*, respectively; *RB* and *RC* are the output reliability of *g* and the circuit reliability, respectively; *PO* is the primary output.

All the above operations are performed on elements with identical coding. The operations of the binary coding are mainly used to guide the operations of the corresponding decimal coding, and the binary coding is used to judge the legality of the corresponding decimal coding. The above operations mainly involve two-sided contents: code the primary input signals and circuit units with binary-decimal coding, and perform the operations between the elements with a different type of coding.

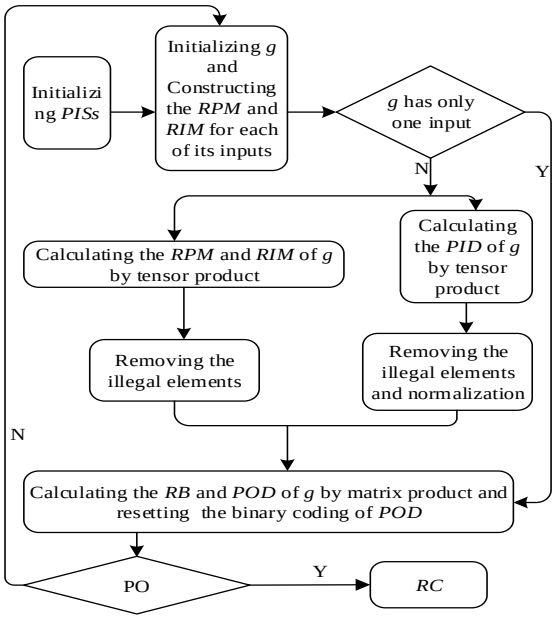

FIGURE 1. The calculation process for the EPTM model

a) Hybrid coding

The four available states for each primary input signal can be completely exhibited by a 2-bit binary coding as follows: 00 is a non-signal input; 01 and 10 are the normal signal inputs; 11 is an illegal signal. For a circuit with *m* primary inputs, the length of its binary coding is 2*m* in accordance with the order from low-bit to high-bit. The decimal coding is the probability of the input state. For example, supposing a circuit with *m* primary inputs, its initializations are shown in Fig. 2 and Fig. 3 when the fault probability of its *i*th input signal is ps_i, and the fault probability of its *j*th circuit unit, denoted as NAND-2, is p_j.

$$\begin{array}{c} \\ 0 \\ 1 \end{array}\begin{bmatrix} \overset{0}{00\cdots01\cdots00}, & 1\text{-}ps_i, & \overset{1}{00\cdots01\cdots00}, & ps_i \\ \underset{m}{00\cdots10\cdots00}, & ps_i, & \underset{m}{00\cdots10\cdots00}, & 1\text{-}ps_i \end{bmatrix}$$

FIGURE 2. Coding of the ith primary input signal

$$\begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array}\begin{bmatrix} \overset{0}{00\cdots00\cdots00}, & p_j, & \overset{1}{00\cdots00\cdots00}, & 1\text{-}p_j \\ \underset{m}{00\cdots00\cdots00}, & p_j, & \underset{m}{00\cdots00\cdots00}, & 1\text{-}p_j \\ \underset{m}{00\cdots00\cdots00}, & p_j, & \underset{m}{00\cdots00\cdots00}, & 1\text{-}p_j \\ \underset{m}{00\cdots00\cdots00}, & 1\text{-}p_j, & \underset{m}{00\cdots00\cdots00}, & p_j \end{bmatrix}$$

FIGURE 3. Coding of the jth circuit unit

b) Numerical calculation

As the basic computing unit, the circuit units mainly involve multiplication, which includes the multiplications of the binary coding and decimal coding. For the elements of (Eb_1, Ed_1) and (Eb_1, Ed_1), the multiplication relationship between them can be expressed as Equation (1), where Eb_i and Ed_i are the binary coding and decimal coding of the *i*th element, respectively.

$$(Eb_1, Ed_1)\times(Eb_2, Ed_2)=(Eb_1|Eb_2, Ed_1\times Ed_2) \quad (1)$$

B. Quantitative importance for circuit units

To quantify the importance of the circuit units by the results obtained from section II.A, the following three works need to be further studied. First, construct a quantization model for the reliability gradient of the circuit units associated with their topological locations. Second, propose a self-adaptive and effective algorithm to calculate the sensitized path coverage rate of the circuit units. Third, provide a reasonable measurement method to sort the importance of circuit units.

a) Reliability gradient for circuit units

The reliability gradient (denoted as ε) reflects the effect of circuit units on the circuit structure reliability [18, 19]. The following two goals need to be achieved in its quantification. First, the calculation needs to be able to be performed in circuit design. Second, the stability of the results needs to be guaranteed for comparison purposes. The analysis found that ε is related to the reliability increment of the circuit unit (denoted as ΔUR) and directly affected by the input reliability of the circuit unit (denoted as *URI*). Because the EPTM model

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2800712, IEEE Access

can be used to calculate the output reliability of the modules between the primary inputs and any leads [16], the ΔUR of a circuit unit can be obtained by subtracting the output reliability of its pre-stage lead *URI* from the reliability of its post-stage lead *URO*. ΔUR reflects the effect of the circuit topological structure and the topological location of the circuit unit on the calculated result, and it does not change with extended sensitized paths. Therefore, the requested ε can be obtained by Equation (2) based on the gradient theory [19].

$$\varepsilon = \frac{\Delta UR}{URI} \tag{2}$$

However, the representative circuit units in several-abstract-level circuits tend to have input-output relations (as shown in Fig. 4), i.e., a circuit unit is usually in multiple sensitized paths, so all εs for different sensitized paths should be calculated according to the gradient theory. Because the reliability of a circuit is determined by its weak units, ε for the circuit in Fig. 4 is considered equal to the minimum of all εs according to the barrel theory. Therefore, Equation (2) can be rewritten as Equation (3) to satisfy the requirement of calculating the ε of the circuit unit presented in Fig. 4, where $h \in \{\ldots, i, \ldots, j, \ldots\}$, $t \in \{\ldots, i, \ldots, j, \ldots, k, \ldots\}$.

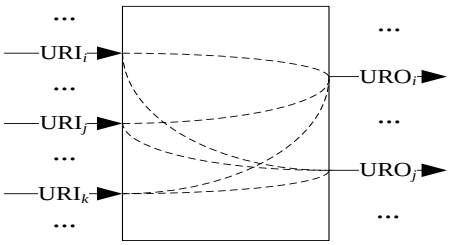

FIGURE 4. A representative circuit unit

$$\varepsilon = \begin{cases} MIN\left(\dfrac{URO_h - URI_t}{URI_t}\right), & if \ \ URO_h > URI_t \\ 0, & if \ \ URO_h = URI_t \\ -MAX\left(\left|\dfrac{URO_h - URI_t}{URI_t}\right|\right), & if \ \ URO_h < URI_t \end{cases} \tag{3}$$

Equation (3) reflects the increment effect of the circuit unit to the circuit structure reliability by ΔUR. It also reflects the base effect of the circuit unit on its sensitized paths by *URI* and meets the requirements, the stability of the results and the dynamic of the process, for the calculation of ε. Therefore, it is reasonable to measure ε using Equation (3).

What is the relationship between ε for a circuit unit and its importance ordering? The analysis found the correspondence between the output reliability trend in any leads and the corresponding ε tread, as shown in Fig. 5. Evidently, there is a negative slope between the different *R*s corresponding to the pre-stage lead and the post-stage lead for a circuit unit. In addition, a greater reliability fluctuation corresponds to a smaller slope, which corresponds to the negative ε of the circuit unit. A larger reliability gradient caused by the circuit unit corresponds to a smaller ε (as shown by the real circles in Fig. 5). Therefore, according to the gradient and barrel theories, ε can be used to measure the importance of circuit units, and the importance ordering of the circuit units is in contrast to ε. However, it is inevitable to encounter circuit units with identical ε (as shown by the square circles in Fig. 5). The analysis found that they exhibited identical weakness but had different effects on the other circuit units. Thus, this paper further measures the importance of circuit units with the same ε.

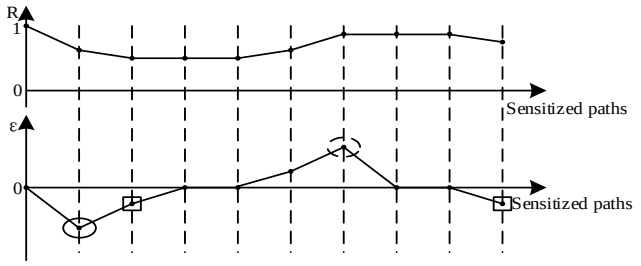

FIGURE 5. Correspondence between the R *tread of a circuit unit and its* $\boldsymbol{\varepsilon}$ *tread on the sensitized paths*

b) Sensitized path coverage rate for circuit units

The sensitized path coverage rate β for the circuit units reflects the effective coverage of a circuit unit to its post-stage circuit units. A larger β implies that more circuit units are covered. It is a key measure to improve the precision of the importance measurement of circuit units by sorting βs for the circuit units with the same ε. The analysis found that a circuit unit could generally reach more circuit units when it is in the smaller layer and has a larger outdegree (outdegree is defined as the number of interconnects starting at a node that is treated as a vertex), which makes it have a larger impact on the other circuit units and usually have a greater β. Therefore, the circuit unit with larger β is more important. Considering the requirements of the computational accuracy and time-space complexity, this paper proposes a self-adaptive calculation method to estimate β for the circuit units using Equations (4) and (5).

$$\beta = \lambda_k \frac{l_n - l_i}{l_n} + \sum_{j=l_i}^{l_{i+k}} \lambda_k \frac{w_j}{w} \tag{4}$$

$$\lambda_k = \frac{1}{k+2} \tag{5}$$

where l_i is the circuit layer number of the circuit unit *g*; l_n is the maximum layer number of the circuit; w_j is the sum of the outdegrees of the circuit units in the *j*th layer that can be reached from g; *w* is the maximum width of the circuit; $k \in \{0, 1 \ldots, n\text{-}i\}$; λ_k is a weighting to satisfy the requirement of $\beta \in [0, 1]$; and *k* is the iterative termination condition and provided by Fig. 6 and algorithm 1. Because the role of β is to differentiate the importance of circuit units with the same ε, we only provide a method to sort βs and do not strictly solve them, which does not affect the accuracy of the final results

and can reduce the computational complexity. On this basis, this paper uses a mean strategy to calculate λ_k.

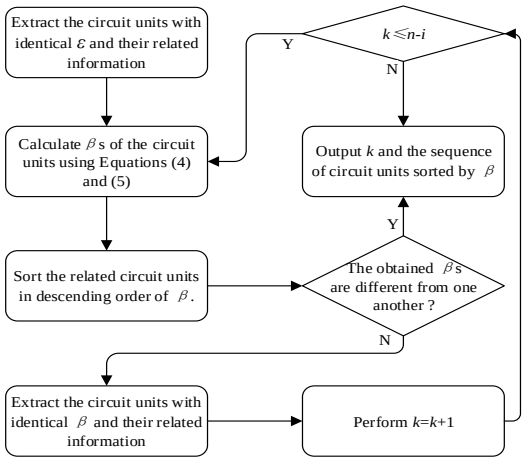

FIGURE 6. Computational flowchart of k

Algorithm 1. Solving for k
Input: circuit units with the same ε
Output: k and an ordered sequence for the circuit units with identical ε
1. Obtain the circuit units with identical ε and extract their layer number, outdegree and basic information.
2. Calculate βs of the circuit units using Equations (4) and (5).
3. Sort the related circuit units in descending order of β, If all obtained βs from step 2 are different from one another, go to step 5.
4. Obtain the circuit units with identical β and their related information, then perform k=k+1. If $k \le n-i$, go to step 2; else, go to step 5.
5. Output k and the sequence of circuit units sorted by β, then exit the algorithm.

In algorithm 1, step 1 traverses the node-list containing N circuit units to extract the required information for the special circuit units with the same ε and stored them, so the time and space complexity of step 1, on average, are approximately $O(N^2/2)$ and $O(N/2)$, respectively. In step 2, the time complexity of the calculation for one circuit unit, on average, are approximately $O[(3^n\text{-}1)/(2n+2)]$. Assuming that half of the circuit units in circuit are the special circuit units with identical ε, the time complexity of the step 2, on average, is approximately $O[N(3^n\text{-}1)/(4n+4)]$. Considering that the calculated results are stored in the memory created in step1, the space complexity of step 2 is expressed as 0. In step 3, the worst case is $k \neq 0$, then a sorting operation should be performed and the time complexity is approximately $O(N^2/4)$, and no new memory is created in this step. In step 4, the worst case is that the calculation lasts until the last layer of the circuit, and the results are stored in the memory created in step 1. Therefore, the time complexity of this step is approximately $O[N(3^n\text{-}1)/8]$. In step 5, the operations have a constant time consumption. In summary, the time complexity of algorithm 1 is approximately $O[(6N^2+N(3^n\text{-}1))/8]$, and its space complexity is approximately $O[N/2]$.

c) Importance of circuit units

Through the above analysis, it can be found that the weak circuit units in reliability can be found based on ε. If they are reinforced, the reliability of blockchain architectures will obviously improve. The specific process is as follows. First, sort the importance of the circuit units in order from large to small according to the corresponding εs. Second, propose a method to accurately estimate the importance of the circuit units by ε and β, where the basis is that the circuit units with larger β can have a greater effect on the circuit reliability than the others for the circuit units with the same ε.

Considering the hierarchy of this method and the result ordering, it is reasonable to measure the importance of circuit units using the sequence comparative method. The main steps are performed as follows. First, initialize the ordered pair $<g, \varepsilon, \beta>$, which indicates the information of the circuit unit and its importance. Second, sort $<g, \varepsilon, \beta>$ by ε from small to large. Third, extract $<g, \varepsilon, \beta>$ with the same ε, calculate β, sort $<g, \varepsilon, \beta>$ again by β in order from large to small, and put the results into the corresponding locations. Finally, extract gs in order. The obtained results are the importance ordering of the circuit units for the circuit.

It is generally assumed in engineering that the simultaneous failure of approximately 5 - 10% of important circuit units will result in the system running badly and even breakdown. Thus, there are no excess circuit units to be focused on, which means that there is a high requirement on the accuracy of the method for measuring the importance of circuit units. Further analysis found that, besides locating the important circuit units, the method could also be used to locate the circuit units with high reliability-tolerance to reduce the manufacturing cost. Unlike the important circuit units, they generally have large ε (as shown by the virtual circles in Fig. 5).

C. Measurement algorithm for the importance of circuit units

To dynamically measure the importance of circuit units based on the proposed method, the following steps are performed layer by layer for the given circuit. First, calculate the output reliability for the circuit units using the method presented in section II.A. Second, calculate the ε of the corresponding circuit units using the method presented in section II.B.A until the circuit primary outputs are reached. Third, calculate β for the circuit units with the same ε using the method presented in section II.B.B. Finally, sort the importance of the circuit units using the sequence comparative method presented in section II.B.C.

Algorithm 2. The importance measurement of circuit units
Input: circuit netlist
Output: an importance-based ordered sequence for the circuit units

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2800712, IEEE Access

1. Parse the circuit netlist and initialize the relevant parameters.
   1) Layer the circuit using the method in Ref. [20] and extract the relevant parameters. Extract the numbers of primary inputs, primary outputs and circuit units and the maximum width for the circuit, which are denoted as *pn*, *pm*, *N* and *w*, respectively; identify the layer for the circuit by number, denoted as l_i (i=0, 1, ⋯, c), and initialize the circuit units by ordered pair, expressed as <g_j, 0, 0> (j=1, 2, ⋯, N).
   2) Code the primary input signals and circuit units using the method presented in section II.A.
2. Calculate the output reliability of the circuit unit g_k in the l_ith level and provide its ordered pair <g_k, ε_k, 0>.
   1) Construct the input reliability matrix and ideal input matrix for each input of g_k using the method in section II.A and calculate its input probability distribution, input reliability matrix and ideal input matrix.
   2) Check the legality of the results obtained from step (2.1), remove the illegal elements based on the computational rules in section II.A, and maintain their order.
   3) Calculate the output reliability and output probability distribution of g_k using the method in section II.A.
   4) Calculate ε_k of g_k using Equation (3) and update <g_k, 0, 0> with <g_k, ε_k, 0>.
3. Output the ordered sequence of the circuit units according to their importance.
   1) Sort <g, ε, 0> by ε from small to large.
   2) Sort <g, ε, 0> with the same ε using Algorithm 1 and put the results into the locations created in step (3.1).
   3) Obtain g from the ordered pairs, which are updated in step (3.2), and construct an importance-based ordered sequence for the circuit units according to people's requirement.

In algorithm 2, step 1 initializes and stores the relevant parameters in units of basic gates during netlist parsing, so the time-space complexity of step 1 can be approximately O(N). In step 2, although there are matrix operations, they are always implemented in units of basic gates and the corresponding results are stored in the memory created in step 1. Therefore, the time complexity of this step can be expressed as $O(N)$. In step 3, a sorting algorithm and algorithm 1 are implemented and no new memory is created in this step, so the time complexity is approximately O($(8N^2+ N(3^n-1))/8$). In summary, the time complexity of algorithm 2 is approximately O($N(3^n+N)$), and its space complexity is approximately O(N).

Fig. 7 is an application example for the proposed algorithm 2. For convenience and without loss of generality, this paper assumes that the primary input signals are in the ideal state and obey the uniform distribution. Unless otherwise stated, all circuit units have identical fault probability p. When p = 0.01, the output reliability treads for the representative sensitized paths in Fig. 7 (such as route A: $g_4 \rightarrow g_6$; route B: $g_1 \rightarrow g_3 \rightarrow g_4 \rightarrow g_6$; route C: $g_1 \rightarrow g_7$) were provided using Algorithm 2, and the comparable ε for each circuit unit was also provided; the results are shown in Fig. 8, where *R*-out refers to the output reliability for the circuit unit.

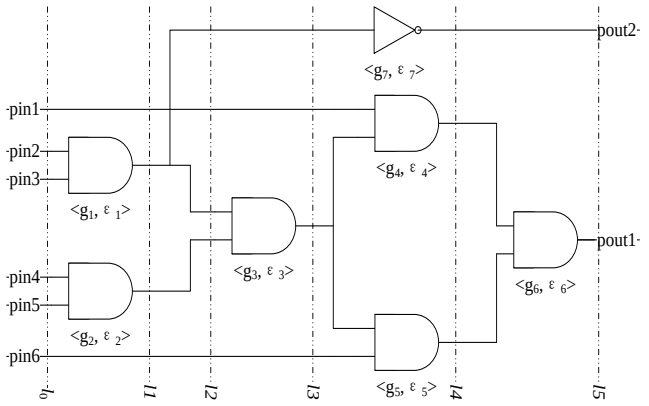

FIGURE 7. Example of a gate-level circuit

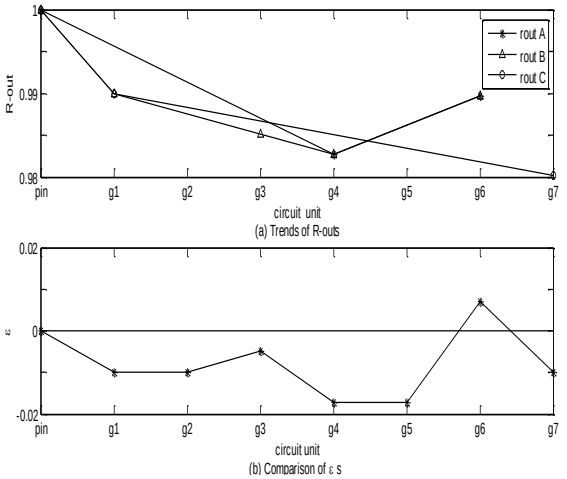

*FIGURE 8. Comparison of **ε**s for the circuit units in Fig. 7*

Fig. 8 shows that the weak circuit units can be pinpointed by ε, such as g_4 and g_5, but it cannot further provide the importance ordering of the circuit units with the same ε, such as g_1 and g_2, g_4 and g_5. Using the strategy in step 3 of Algorithm 2, we find that the importance of g_1 is larger than that of g_2 in Fig. 7 and that the importance of g_4 is equal to that of g_5 because they are perfectly symmetric. The results were also verified by the experiment shown in Fig. 10.

III. Experimental Evaluations

To verify the effectiveness of the proposed method, simulations were performed using a computer with a 3.2-GHz processor and 4 GB RAM. Some typical circuits [16] with different abstract levels (such as the transistor level, gate level and register transfer level) were used in the experiment. The experimental results for the circuits, such as NAND-2, NOR-2, NOR, C17, Fig. 7's circuit, a decoder and an adder, were obtained using the proposed method and the Monte Carlo method, and the results are shown in Table 1. However, the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2800712, IEEE Access

experiments face two obstacles. First, the Monte Carlo method has unbearable time consumption. Second, circuit netlists cannot effectively provide human-readable identities for circuit units, which hinders the verification of the importance ordering results for the circuit units. Thus, an operational strategy is designed to avoid these obstacles as follows. First, identify the most important circuit unit using the proposed method. Second, measure the importance of the circuit unit identified by the first step and the circuit units selected randomly using the Monte Carlo method. Finally, compare the results obtained from the second step. If the importance levels of the circuit units selected randomly are no more than that of the circuit unit identified by the first step, it can be concluded that the results of the proposed method are reasonable based on the random set theory [21].

To clarify, all primary input signals are in the ideal state and obey the uniform distribution unless otherwise stated. Furthermore, according to the principle of small samples [22], 10 circuit units are randomly selected to perform in the experiments for the circuits with 10 or more circuit units; otherwise, all circuit units are selected.

Table 1 clearly shows that the proposed method and Monte Carlo method have equivalent results. The proposed method runs faster than the Monte Carlo method, but their memory consumptions are similar. The reasons can be analyzed from the following two perspectives.

First is measurement precision. The proposed method calculates the output reliability for each output lead in the circuit based on the weak equivalence principle and the virtual method to guarantee the precision of their output results. In addition, it also measures the importance of the circuit units based on the gradient and barrel theories and the compensation strategy to quantify the base effect and increment effect on the results.

TABLE I
COMPARISON OF THE RESULTS OBTAINED BY THE PROPOSED METHOD AND THE MONTE CARLO METHOD (P = 0.01)

Abstraction level	Circuits	Matching results	Time /s		Memory /MB	
			The proposed method	MC	The proposed method	MC
Transistor level	Nand-2	1	0.087	7.41	0.60	0.58
	Nor-2	1	0.088	7.39	0.59	0.58
	Not	1	0.047	3.89	0	0
Gate level	C17	1	0.100	11.56	0.63	0.63
	Fig. 7	1	0.113	12.03	0.62	0.59
	Comparator	1	0.207	18.12	0.79	0.75
RTL level	multiplexer	1	0.289	15.63	0.66	0.62
	adder	1	0.324	14.877	0.67	0.65
	encoder	1	0.185	12.72	0.65	0.60

Second is time-space complexity. Using the binary-decimal coding strategy, the output reliabilities in any leads are iteratively calculated in units of circuit units, and the importance of the circuit units is measured at the same time. Thus, similar to the method proposed in Ref. [16], the proposed method also has a small time-space consumption. The importance of the circuit units is also measured by the Monte Carlo method in units of circuit units. Although an optimal sampling policy is performed, multiple samples are also to be considered, and each one had exponential computational complexity to simulate the faults and the input probability distribution for circuits. Furthermore, except for the circuit structure information, only the analogue functions for the current experimental samples reside in the memory. Therefore, the Monte Carlo method has exponential time consumption and linearized memory consumption for the important measurement of circuit units.

The importance ordering for circuit units is affected by the faults of other circuit units on their sensitized paths in the experiment. For example, for the five schemes based on the different fault probabilities of circuit units ps in Fig. 7 circuit (which are presented as follows: Scheme A: $p1 = p2 = p3 = p4 = p5 = p6 = p7 = 0$; Scheme B: $p1 = p2 = p3 = p4 = p5 = p6 = p7 = 0.005$; Scheme C: $p1 = p2 = 0.02$, $p3 = p4 = 0.001$, $p5 = p6 = p7 = 0.02$; Scheme D: $p1 = p2 = p3 = 0.02$, $p4 = p5 = p6 = p7 = 0.001$; Scheme E: $p1 = p2 = p3 = p4 = 0.001$, $p5 = p6 = p7 = 0.02$), the importance ordering for the circuit units was provided using the proposed method, as shown in Fig. 9, which shows that ε of the circuit units is changed in different schemes, where p_i is the fault probability of the circuit unit g_i (i=1, 2, ⋯, 7), $\beta_4=\beta_5$, and $\beta_1>\beta_2$.

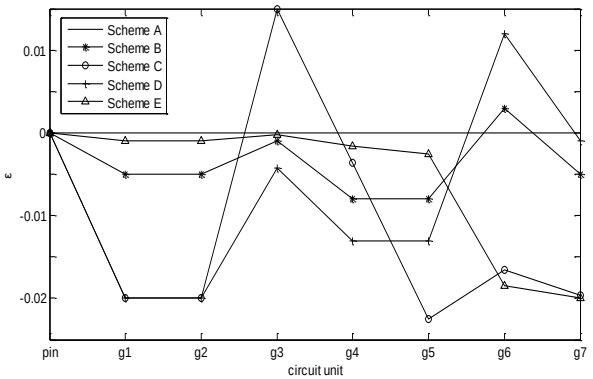

FIGURE 9. Comparison of the change in ε of the circuit units in Fig. 7 circuit in different schemes

Fig. 9 shows that the importance ordering of circuit units in Fig. 7 has different results in different schemes. For example,

in the ideal case (such as Scheme A), the importance of each circuit unit is identical; when the fault probability of each circuit unit is identical (such as Scheme B), the importance ordering of the circuit units is (g_4, g_5) > g_1 > g_2 > g_7 > g_3 > g_6; otherwise (such as Scheme C/D/E), they have other importance orderings. The analysis found that these results are affected by the circuit topology structure (such as Scheme B), the fault conditions of the circuit units themselves (such as Scheme E), and their related circuit units (such as Scheme C/D). Therefore, to accurately quantify the importance of circuit units, both the practical application environment of the circuit and the associated faults among the circuit units should be considered.

Using the results obtained from the proposed method, the important circuit units can be selectively reinforced to significantly improve the circuit reliability at a small cost. For example, in Fig. 7 circuit, when each circuit unit has identical fault probability p = 0.05 (marked as the Basic scheme), the importance ordering of the circuit units is: (g_4, g_5) > g_1 > g_2 > g_7 > g_3 > g_6. For this scheme, four reinforcement schemes are used to improve the circuit reliability: Scheme F: $p1 = p2 = p3 = 0.05$, $p4 = p5 = 0.01$, $p6 = p7 = 0.05$; Scheme G: $p1 = 0.01$, $p2 = p3 = p4 = p5 = p6 = p7 = 0.05$; Scheme H: $p1 = 0.01$, $p2 = p3 = 0.05$, $p4 = p5 = 0.01$, $p6 = p7 = 0.05$; Scheme I: $p1 = p2 = p3 = p4 = p5 = p6 = p7 = 0.01$. The improved effects are compared in Fig. 10.

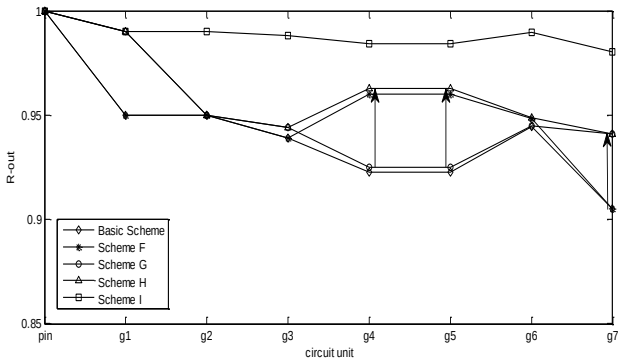

FIGURE 10. Comparison of the improved effects for the reliability of Fig. 7 circuit in different reinforcement schemes

It can be seen from Fig. 10 that the weakness of Fig. 7 circuit mainly concentrates in g_4, g_5 and g_7 for the Basic Scheme. Through Scheme F and Scheme G, the circuit reliability is not significantly improved. For example, the output reliability of g_7 remains unchanged in Scheme F; the output reliabilities of g_4 and g_5 yield no obvious improvement in Scheme G. However, in Scheme H and Scheme I, the circuit reliability is significantly improved, and the output reliabilities of g_4, g_5 and g_7 are evidently improved. These results mainly depend on the reinforcement schemes. For example, Scheme I reinforces all circuit units in Fig. 7 circuit, which could significantly improve the circuit reliability but there is a high cost. Thus, it is not recommended for adoption except in a special application environment. In Scheme H, the first three important circuit units are selected to reinforce, which significantly improves the circuit reliability at a small cost. The reinforcement target in Scheme G is the most important circuit unit g_1 in the sensitized path $g_1 \rightarrow g_7$, which can significantly improve the output reliability of g_7 but does not obviously improve the output reliabilities of g_4 and g_5 in the sensitized paths $g_1 \rightarrow g_3 \rightarrow g_4 \rightarrow g_6$ and $g_2 \rightarrow g_3 \rightarrow g_5 \rightarrow g_6$, respectively. Scheme F has similar results. Therefore, the number of circuit units selected to reinforce in the circuit design depends on the practical requirements.

IV. Conclusions

To measure the importance of circuit units efficiently, this paper calculates the output reliabilities in any leads using the EPTM model and provides a calculation method for the reliability gradient of circuit units at several abstraction levels. Next, a self-adapted and effective algorithm is proposed to calculate the sensitized path coverage rate for the circuit units with the same reliability gradients to further sort their importance. Combining the two-level metrics and using the sequence comparative method, a dynamic measurement algorithm with small time-space consumption is constructed to measure the importance of circuit units. The theoretical analysis and simulation results on typical circuits show that the proposed method has high calculation accuracy. Further analysis and simulation show that this method has great maneuverability and will play an important role in the design of miniature and highly reliable circuits, which facilitates the operations of blockchains in a reliable hardware environment, thereby enhancing the security and privacy of blockchains.

ACKNOWLEDGMENT

Financial support for the study was provided by the National Natural Science Foundation of China (Nos. No. 61502422, 61772199, 61772198, 61432017, 61503338 and 61773348), the Natural Science Foundation of Zhejiang Province (Nos. LY18F020028, LQ15F020006, LY18F020031, LY18F030023 and LY17F030016) and the Natural Science Foundation of Zhejiang University of Technology (No. 2014XY007).

REFERENCES

[1] ZHENG Z, XIE S, DAI H, et al. Blockchain challenges and opportunities: A survey [J]. International Journal of Web and Grid Services, 2016, 2016(1): 1-25.

[2] LIN I-C, LIAO T-C. A Survey of Blockchain Security Issues and Challenges [J]. International Journal of Network Security, 2017, 19(5): 653-659.

[3] PANICKER S, PATIL V, KULKARNI D. An Overview of Blockchain Architecture and it's Applications [J]. International Journal of Innovative Research in Science, Engineering and Technology, 2016, 5(11): 20074-20084.

[4] KISHIGAMI J, FUJIMURA S, WATANABE H, et al. The Blockchain-Based Digital Content Distribution System [M]. 2015 IEEE Fifth International Conference on Big Data and Cloud Computing. Dalian, China; IEEE Xplore. 2015: 187-190.

[5] LI J, LIANG G, LIU T. A Novel Multi-link Integrated

Factor Algorithm Considering Node Trust Degree for Blockchain-based Communication [J]. KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS, 2017, 11(8): 3766-3788.

[6] TOSH D K, SHETTY S, LIANG X, et al. Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack [M]. IEEE/ACM International Symposium on Cluster. Madrid, Spain; IEEE Xplore. 2017: 1-10.

[7] TOSH D K, SHETTY S, LIANG X, et al. Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack [M]. The 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. Madrid, Spain; IEEE Press. 2017: 458-467.

[8] XIAO J, JIANG J, LIANG J. Transistor-level Oriented Calculation of Reliability for Generalized Gates Based on PTM [J]. SCIENCE CHINA Information Sciences, 2014, 44(10): 1226-1238.

[9] CHIEN-CHIH Y. Probabilistic Analysis for Modeling and Simulating Digital Circuits [D]. Michigan; The University of Michigan, 2012.

[10] DANIEL S, SWARZ R. Reliable Computer Systems: Design and Evaluatuion [M]. New Zealand: Digital Press, 2014.

[11] CALOMARDE A, AMAT E, MOLL F, et al. SET and noise fault tolerant circuit design techniques: Application to 7nm FinFET [J]. Microelectronics Reliability, 2014, 54(4): 738-745.

[12] PAREEK V. A New Gate for Optimal Fault Tolerant & Testable Reversible Sequential Circuit Design [D]. Kota; Rajasthan Technical University, 2014.

[13] LEE P A, ANDERSON T. Fault tolerance: principles and practice [M]. Berlin: Springer Science & Business Media, 2012.

[14] WANG L, WU C, WEN X. VLSI test principles and architectures [M]. Burlington: Elsevier Morgan Kaufmann Publishers, 2006.

[15] INOUE H. Semiconductor integrated circuit, circuit testing system, circuit testing unit, and circuit test method: US, 8,872,537 [P/OL]. 2014-10-28

[16] XIAO J, LEE W, JIANG J, et al. Circuit reliability estimation based on an iterative PTM model with hybrid coding [J]. Microelectronics Journal, 2016, 52(4): 117-123.

[17] KRISHNASWAMY S, VIAMONTES G F, MARKOV I L, et al. Accurate reliability evaluation and enhancement via probabilistic transfer matrices; proceedings of the Design, Automation and Test in Europe, F, 2005 [C]. IEEE.

[18] XIAO J, JIANG J, ZHU X. A Method of Circuit Reliability Estimation Based on Iterative PTM Model [J]. Chinese Journal of Computers, 2014, 37(7): 1508-1520.

[19] KELLEY H J. Gradient theory of optimal flight paths [J]. Ars Journal, 1960, 30(10): 947-954.

[20] MICHAEL B, D A V. Essentials of electronic testing for digital, memory and mixed-signal VLSI circuits [M]. Dordrecht: Springer Science & Business Media, 2000.

[21] GOUTSIAS J, MAHLER R P S, NGUYEN H T. Random sets: theory and applications [M]. Berlin: Springer Science & Business Media, 2012.

[22] LIESE F, MIESCKE K-J. Statistical Decision Theory: Estimation, Testing, and Selection [M]. New York: Springer, 2008.

Jie Xiao received his Ph.D. degree in computer system architecture from Tongji University, Shanghai, China, in 2013. He is currently working with the department of computer science and technology, Zhejiang University of Technology, Hangzhou, China. His current research interests include reliability evaluation and fault-tolerant design, blockchain security, deep learning and combinatorial optimization-computation. He also serves as a consultant and technical adviser for a research institute in electronic information fields. E-mail: xiaojiexqj@foxmail.com.

Jungang Lou received the B.S. degree in Mathematics from Zhejiang Normal University, China, in2003, and the M.Sc. degree in computational mathematics and the Ph.D. degree in computer software and theory from Tongji University, Shanghai, China, in 2006 and 2010, respectively. He is currently an Associate Professor with the School of Information Engineering, Huzhou University, Huzhou, China. He also holds a postdoctoral position at the Institute of Cyber-Systems and Control, Department of Control Science and Engineering, Zhejiang University, Zhejiang, China. He is now also a Visiting Scholar with the department of Computer Science at the University of Texas at San Antonio between Nov. 2017 and May 2018. His current research interests include dependable computing, reliability engineering, computer system performance evaluation, neural network optimization, and time series prediction.

Jianhui Jiang received his BE, ME and PhD degrees in 1985, 1988, and 1999, respectively. He is currently a full professor of software engineering and Vice Dean of the School of Software Engineering at Tongji University. He is Vice Director of Technical Committee on Fault-tolerant Computing, Chinese Computer Federation (CCF). He has served on several program committees of national or international symposiums or workshops including IEEE Pacific Rim International Symposium on Dependable Computing, IEEE Asian Test Symposium, IEEE Workshop on RTL and High Level Testing. He has co-authored two books and published more than 180 technical papers. His current research interests include dependable systems and networks, software reliability engineering, VLSI/SoC test-ing and fault-tolerance. He is a senior member of CCF.

Xiaoxin Li, received the PhD degree in computer application technology from South China University of Technology, Guangzhou, China, in 2009. Since then, he has been a postdoctoral researcher in the Department of Mathematics,

Faculty of Mathematics and Computing, Sun Yat-Sen University, Guangzhou, China. He joined Zhejiang University of Technology, Hangzhou, China, in 2013. His current research interests include deep learning, error coding, and image analysis.

Xuhua Yang, received his B.E. degree in Automation from China University of Petroleum, Dongying, China, in 1993; and received his M.S.degree and Ph.D. degree in control science and engineering from Zhejiang University,Hangzhou, China, in 2001 and 2004, respectively. He is currently a Professor with Computer Science and Technology, Zhejiang University of Technology, Hangzhou, China. His current research interests include artificial intelligent, complex network system, intelligent transportation sytem, link prediction, and deep learning.

Yujiao Huang, received the B.S. degree in information and computer science, the M.S. degree in computational mathematics and the Ph.D. degree in control theory and control engineering from Northeastern University, Shenyang, China, in 2008, 2010 and 2014, respectively. She is now a lecturer at Zhejiang University of Technology. Her research interests are in areas of artificial neural networks, stability theory, and dynamical systems.