9200100006881011101000039850000000

특허출원서

【참조번호】 P190068KR02

【출원구분】 특허출원

【출원인】

【명칭】 광주과학기술원

【특허고객번호】 3-1998-099381-5

【대리인】

【성명】 김기문

【대리인번호】 9-2001-000068-8

【포괄위임등록번호】 2015-044266-2

【발명의 국문명칭】 블록체인의 거래검증시스템, 및 블록체인이 거래검증방법

【발명의 영문명칭】 Bargain authentification system and method for the block chain

【발명자】

【성명의 국문표기】 장재혁

【성명의 영문표기】 JANG, JE HYUK

【주민등록번호】 890921-1677213

【우편번호】 61005

【주소】 광주광역시 북구 첨단과기로 123(오룡동) 광주과학기술원 전기전자컴퓨터공학부

【발명자】

【성명의 국문표기】 이흥노

【성명의 영문표기】 LEE, HEUNG NO

【주민등록번호】 661120-1018916

【우편번호】 61005

【주소】 광주광역시 북구 첨단과기로 123(오룡동) 광주과학기술원
전기전자컴퓨터공학부

【출원언어】 국어

【우선권주장】

【출원국명】 KR

【출원번호】 10-2019-0061493

【출원일자】 2019.05.24

【증명서류】 미첨부

【심사청구】 청구

【공지예외적용대상증명서류의 내용】

【공개형태】 논문발표

【공개일자】 2019.03.05

【이 발명을 지원한 국가연구개발사업】

【과제고유번호】 1711093581(NN24010)

【부처명】 과학기술정보통신부

【연구관리전문기관】 정보통신기술진흥센터

【연구사업명】 융합기술개발

【연구과제명】 확장가능한 탈중앙화 보안성 ECCPoW 블록체인

【기여율】 1/2

【주관기관】 광주과학기술원

【연구기간】 2019.04.01 ~ 2019.12.31

【이 발명을 지원한 국가연구개발사업】

【과제고유번호】 GK11380

【부처명】 광주과학기술원

【연구관리전문기관】 광주과학기술원

【연구사업명】 실용화연구개발

【연구과제명】 암호-부호 작업증명(PoW) 비트코인/이더리움 하드포크
1.0개발

【기여율】 1/2

【주관기관】 광주과학기술원

【연구기간】 2019.02.01 ~ 2019.12.31

위와 같이 특허청장에게 제출합니다.

대리인 김기문 (서명 또는 인)

【수수료】

【기본출원료】	0	면	46,000 원
【가산출원료】	37	면	0 원
【우선권주장료】	1	건	18,000 원
【심사청구료】	13	항	715,000 원
【합계】			779,000 원

【감면사유】 정부출연연구기관(50%감면)[1]

【감면후 수수료】 398,500 원

【첨부서류】 1.공지예외적용대상(신규성상실의예외, 출원시의특례)규정을 적용받기 위한 증명서류_1통

Profitable Double-Spending Attacks

Jehyuk Jang, Heung-No Lee

(Submitted on 5 Mar 2019 (v1), last revised 9 Apr 2019 (this version, v2))

Our aim in this paper is to investigate the profitability of double-spending (DS) attacks that manipulate a priori mined transaction in a blockchain. Up to date, it was understood that the requirement for successful DS attacks is to occupy a higher proportion of computing power than a target network's proportion; i.e., to occupy more than 51% proportion of computing power. On the contrary, we show that DS attacks using less than 50% proportion of computing power can also be vulnerable. Namely, DS attacks using any proportion of computing power can occur as long as the chance to making a good profit is there; i.e., revenue of an attack is greater than the cost of launching it. We have novel probability theory based derivations for calculating time finite attack probability. This can be used to size up the resource needed to calculate the revenue and the cost. The results enable us to derive sufficient and necessary conditions on the value of a target transaction which make DS attacks for any proportion of computing power profitable. They can also be used to assess the risk of one's transaction by checking whether or not the transaction value satisfies the conditions for profitable DS attacks. Two examples are provided in which we evaluate the attack resources and the conditions for profitable DS attacks given 35% proportion of computing power against Syscoin and BitcoinCash networks, and quantitatively shown how vulnerable they are.

Comments: 13 pages, 1 figure. Submitted to IEEE Transactions on Information Forensics and Security. Table 1 Has been corrected
Subjects: **Cryptography and Security (cs.CR)**
Cite as: **arXiv:1903.01711 [cs.CR]**
(or **arXiv:1903.01711v2 [cs.CR]** for this version)

Submission history

From: Jehyuk Jang [view email]
[v1] Tue, 5 Mar 2019 07:44:41 UTC (1,156 KB)
[v2] Tue, 9 Apr 2019 03:16:49 UTC (1,105 KB)

Profitable Double-Spending Attacks

Jehyuk Jang and Heung-No Lee, *Senior Member, IEEE*

***Abstract*—Our aim in this paper is to investigate the profitability of double-spending (DS) attacks that manipulate a priori mined transaction in a blockchain. Up to date, it was understood that the requirement for successful DS attacks is to occupy a higher proportion of computing power than a target network's proportion; i.e., to occupy more than 51% proportion of computing power. On the contrary, we show that DS attacks using less than 50% proportion of computing power can also be vulnerable. Namely, DS attacks using any proportion of computing power can occur as long as the chance to making a good profit is there; i.e., revenue of an attack is greater than the cost of launching it. We have novel probability theory based derivations for calculating time finite attack probability. This can be used to size up the resource needed to calculate the revenue and the cost. The results enable us to derive sufficient and necessary conditions on the value of a target transaction which make DS attacks for any proportion of computing power profitable. They can also be used to assess the risk of one's transaction by checking whether or not the transaction value satisfies the conditions for profitable DS attacks. Two examples are provided in which we evaluate the attack resources and the conditions for profitable DS attacks given 35% proportion of computing power against *Syscoin* and *BitcoinCash* networks, and quantitatively shown how vulnerable they are.**

***Index Terms*— Blockchain, Bitcoin, Double-Spending Attack, Profit, Gambler's Ruin Theorem, Poisson Counting Process.**

I. Introduction

A blockchain is a distributed ledger which has originated from a desire to find a novel alternative to centralized ledgers such as transactions through third parties [1]. Besides the role as a ledger, a blockchain has been applied to many areas, e.g., managing the access authority to shared data in the cloud network [2] and averting collusion in e-Auction [3]. In a blockchain network based on the proof-of-work (PoW) mechanism, each peer node who ever has downloaded and installed the pertinent full blockchain protocol suite can join as a full node for the network. Full nodes, or the so-called miners, verify transactions, put them into a block, and mold the block to a chain by solving a cryptographic puzzle. Specifically, a transaction is put into a block by a single full node which solves the cryptographic puzzle for the first time among all full nodes in competition. The reward of minting a certain amount of coins and paid to its own address is given to the first puzzle solver as motivation to join and remain in the network. As a result, transactions are verified by many decentralized full nodes in the network. A number of other researchers [4], [5], [6] have analyzed the winning of rewards under various specific assumptions using game theory.

A consensus mechanism is programmed for decentralized peers in a network to share a common chain. If a full node succeeds in generating a new block, he/she has the latest version of the chain. All of the nodes in the network continuously communicate with each other to share the latest chain. If a node suffers from a conflict between two or more different chains, the consensus rule provides a rule that a single chain is selected. Satoshi Nakamoto suggested the *longest chain consensus* for *Bitcoin* protocol which conserves the longest chain among the conflictions [1]. There are also other consensus rules [7], e.g., GHOST [8].

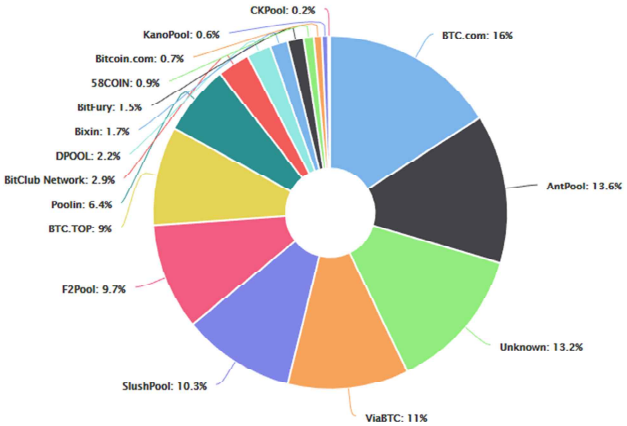

Fig. 1. Computation power distribution among the largest mining pools provided by *blockchain.com* (date accessed: 22 Oct. 2018).

Blockchains are motivated by the trust enabled by decentralized nodes. However, the decentralization mechanism is unfortunately prone to break down [9]. The PoW race is for a full node game of solving a cryptographic puzzle faster than others. As such, a node may form a pool of computing chips to increase the chance to win the PoW race. The problem is that a very limited number of pools occupy a major proportion of the computing power which operates the network. For example, the pie chart shown in Fig. 1 illustrates the proportion of computing power in the Bitcoin network as of October 2018. In the chart, five pools such as BTC.com, AntPool, ViaBTC, F2Pool, and BTC.TOP occupy a dominant proportion of the computing power. That is to say, they have recentralized the Bitcoin network [10].

Double-spending (DS) is one type of attacks made easily probable in a recentralized network. Since a few full nodes can easily occupy a sufficient proportion of computing power of the blockchain network, they are able to manipulate already confirmed transactions. Suppose that a public chain contains a *target transaction* which transfers the ownership of a certain amount of cryptocurrency from the attacker to a merchant for the price of a certain goods and service. Before shipping the goods, a careful merchant will wait until the transaction has been verified in a number of block confirmations by normal peers. We call this process *block confirmation*. At the same time, an attacker with a high computing power confidentially develops a fraudulent chain

The authors are with the School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology (GIST), Rep. of Korea. The asterisk * indicates the corresponding author. The e-mail addresses of authors are (jjh2014@gist.ac.kr, heungno@gist.ac.kr).

aimed at nullifying the target transaction in the public chain. After obtaining the block confirmation and making the fraudulent chain longer than the public one, the attacker then publicly announces the fraudulent chain. The consensus rule is to trust the longer chain, so the normal miners accept the fraudulent chain and discard the shorter public chain. Indeed, there have been a number of reports that cryptocurrencies such as *BitcoinGold*, *ZenCash*, *Zcash*, and *Litecoin Cash* suffered from DS attacks and millions of US dollars were lost in 2018 [11], [12], [13].

Recentralization is not the only concern for DS attacks. The advent of rental services which lend computing equipment for DS attacks can be a major concern as well [14]. Recently, rental services such as *nicehash.com* which provide a brokerage service between the suppliers and the consumers have indeed become available. The concern at hand is then to determine whether or not attacking with a rented computing power really returns a profit. The next concern is to find a strategy for such an attack.

Success by making DS attacks is possible but is believed to be difficult for a public blockchain with a large pool of mining network support. Nakamoto and Rosenfield provided probabilistic results of DS attack success (AS) in [1] and [15], respectively, using gambler's ruin analysis. They showed that the condition guaranteeing for making a successful DS attack is for the attacker to bring in a computing power more than the computing power which is already invested to operate the network; such an attack is thus called 51% attack. This result has been considered as the requirement for AS. This conclusion however shall be reconsidered given our result in the sequel that there are significant chances of making a good profit from DS attacks regardless of the proportion of computing power.

In this paper, our aim is to include profitability and find the requirements for DS attacks to be profitable. In our model, a DS attack succeeds if three conditions are achieved: *i)* block confirmation should be realized; *ii)* the fraudulent chain should be longer than the public chain; and *iii)* both conditions *i)* and *ii)* should be satisfied within a cut time.

A. Contributions

We show that attackers can expect a profitable DS attack not only in the super-50% proportion regime but also in the sub-50% proportion regime where computing power invested by the attacker is smaller than that invested by a target network. A DS attack is profitable if and only if the expectation of a profit function defined in (38) is positive.

To define a profit function, we introduce a novel set of mathematical tools. Specifically, we compute the probability distribution of the time spent for an AS. This AS time incorporates the probability of all possible AS within a *cut time*. The derivation of probability distribution enables us to draw results on expected revenue. Also, the expectation of AS time is used to compute expected expense spent for an attack attempt. As a result, the profit is the difference between the expected revenue and the expected expense.

We show that for a DS attack in the sub-50% proportion regime to be profitable, it is necessary to set the *cut time* to be finite. Otherwise, if an AS never be achieved, infinite deficit can happen. Under any finite *cut time*, we provide a condition on the value of target transaction which suffices a profitable DS attack.

Using these results, we provide examples of resources required for profitable attacks against *BitcoinCash* and *Syscoin,* as of December 2018 (see Section IV-B for details). Suppose that 35% proportion of computing powers is available, and the block confirmation number is 5. To compute the expected expense, we referred to the rental fee of computing power from *nicehash.com*. In the case of *Syscoin*, the expected expense is 1.810 BTC and the required value of the target transaction is 13.134 BTC. The expected AS time is around 9 minutes. In the case of *BitcoinCash*, the expected expense is 2.844 BTC and the required value of the target transaction is 20.639 BTC. The expected AS time is 1 hour 31 minutes.

B. Related Works

References [15] and [16] have analyzed the profitability of DS attacks in terms of revenue and opportunity cost. Opportunity cost is the expected rewards that could be paid out from normal mining and is generally a function of the time spent for an attack attempt. However, Rosenfield assumed the attack time to be a fixed number for the simple calculation of opportunity cost [15], while to simplify the estimation of attack time, Bissias *et al.* included an assumption that the attack stops if either the normal peers or the attacker achieves the block confirmation first [16]. On the contrary, in our model, an attack can be continued indefinitely if it brings a profit, even if the normal peers achieve block confirmation before the attacker does.

Budish conducted simulations on the profitability of DS attacks using more than 50% proportion of computing power [17]. He provided an empirical condition on the value of the target transaction that makes DS attacks not profitable. On the contrary, we consider not only the super-50% proportion regime but also the sub-50% proportion regime. We provide mathematical formulas for the required resources as functions of the computing power and block confirmation number. We also provide practical examples of profitable DS attacks against working blockchain networks.

The web-site *Crypto51.app* lists hourly rental fees for 50% proportion of computing power for the purpose of estimating the profit from DS attacks. However, there is no estimation of the AS time, and thus the estimation of the total cost is absent.

The probability distribution of AS time was analyzed in [18] and [19]. However, none of the results matched with our three conditions for AS. Specifically, neither analysis considered the first condition: *i)* block confirmation should be realized. We compare these results with ours in Section III-D in detail.

C. Organization of the Paper

Section II contains definitions of the three conditions required for a successful DS attack. DS attacks are modeled by the random walk of two independent Poisson counting processes (PCPs). Section III comprises the computation of the probabilities of DS AS and the stochastic behaviors of the first time when the DS attack is successful. In Section IV, we analyze the profitability of DS attacks, followed by providing the resources required to make them profitable. Finally, Section V concludes the paper with a summary.

II. The Attack Model

Here, we define the conditions for a successful DS attack. DS attacks are modeled with two independent PCPs. The PCP events are carefully enumerated to account for the AS.

A. Attack Scenario

We consider blockchain networks which adopt the longest chain consensus. The longest one wins among all of the chains in competition. We assume there are two groups of miners, the normal group of miners and a single attacker. The normal group tends the *public chain*.

When the attacker decides to launch a DS attack, he/she issues a target transaction for the payment of goods or services to transfer the ownership of the cryptocurrency from the attacker him/herself to the victimized counterpart (VC). However, the attacker does not announce the target transaction to the normal group immediately but waits for a new block generation in the public chain. We denote the time at which this new block is generated as $t=0$. At time $t=0$, the attacker announces the target transaction to normal group so that normal group starts to put it into the public chain. At the same time, the attacker makes a fork of the public chain which stems from the newest block generated at $t=0$ and builds it in secret. We refer to this secret fork as *fraudulent chain*. In the fraudulent chain, the target transaction is altered in a way that deceives the counterpart and benefits the attacker; one such an example is to get rid of any record of the target transaction after receiving the goods or services.

Before shipping goods or providing services to the attacker, the VC obviously chooses to wait for a few more blocks in addition to the block on which the target transaction has been entered. The number of blocks the VC chooses to wait for is referred to as the *block confirmation number* $N_{BC}\in\mathbb{Z}^+$ in this paper. Note that the number N_{BC} includes the block on which the target transaction is entered.

The attacker chooses to make the fraudulent chain public if his attack was successful. An attack is successful if the fraudulent chain is longer than the public chain after the moment the block confirmation is satisfied. This is possible because the public chain is always publicly open, while the fraudulent one is kept private by the attacker. However, the attacker will not wait for his success indefinitely since growing the attacker's chain incurs the expense per time spent for operating the computing power. The attack thus stops if the attack does not succeed within a cut time t_{cut} to cut loss.

To sum up, the AS of the DS attack is declared if all of the following conditions $\mathcal{G}^{(1)}$, $\mathcal{G}^{(2)}$, and $\mathcal{G}^{(3)}$ are satisfied.

Definition 1. *A DS attack succeeds if*

1. $\mathcal{G}^{(1)}$: *the length of public chain counting from the moment* $t=0$ *grows greater than or equal to* N_{BC},
2. $\mathcal{G}^{(2)}$: *the length of fraudulent chain counting from the moment* $t=0$ *grows longer than the public chain, and*
3. $\mathcal{G}^{(3)}$: *starting from* $t=0$, *the duration* $T^{(1),(2)}$ *at which both* $\mathcal{G}^{(1)}$ *and* $\mathcal{G}^{(2)}$ *are satisfied for the first time is less than* t_{cut}.

When the cut time of attack is set to infinite $t_{cut}=\infty$, such an attack success is called attack success with the infinite cut time (AS-ICT).

B. The Stochastic Model

We model the length of the public chain and that of the fraudulent chain by two independent PCPs $H(t)$ with parameter λ_H (blocks per second) and $A(t)$ with parameter λ_A, respectively. Both processes start at the zero state $H(0)=A(0)=0$ and independently increase by at most 1 at a time. An increment of 1 in the counting process occurs when the pertinent network adds a new block to its chain and the chain length is grown by 1 unit with each new mining success.

We rewrite the events AS and AS-ICT in terms of $H(t)$ and $A(t)$. In Definition 1, the first two conditions $\mathcal{G}^{(1)}$ and $\mathcal{G}^{(2)}$ are expressed by $H(t)\geq N_{BC}$ and $A(t)>H(t)$, respectively. It is convenient to define the time $T^{(1),(2)}$ at which both $\mathcal{G}^{(1)}$ and $\mathcal{G}^{(2)}$ are satisfied first as follow:

$$T^{(1),(2)}:=\inf\left\{\left\{t\in(0,\infty):H(t)\geq N_{BC};A(t)>H(t)\right\}\cup\{\infty\}\right\}. \quad (1)$$

From the last condition $\mathcal{G}^{(3)}$, the event AS-ICT is declared if $T^{(1),(2)}<\infty$. Similarly, for a finite $t_{cut}<\infty$, the event AS is declared if $T^{(1),(2)}<t_{cut}$.

To simplify $\mathcal{G}^{(1)}$ and $\mathcal{G}^{(2)}$, we form a random walk that represents the difference between $A(t)$ and $H(t)$. For this purpose, we first define two continuous stochastic processes $M(t)$ and $S(t)$, which are respectively defined as

$$M(t):=H(t)+A(t), \quad (2)$$

and

$$S(t):=H(t)-A(t). \quad (3)$$

The first process $M(t)$ is also a PCP [20] with the rate

$$\lambda_T:=\lambda_A+\lambda_H \ \text{(blocks per second)}, \quad (4)$$

which corresponds to the sum of computing powers of the two mining groups. The second process $S(t)$ is the continuous-time analog of a random walk. We define a random walk $S_i\in\mathbb{Z}$ for $i\in\mathbb{Z}^+$ as

$$S_i:=S(T_i), \quad (5)$$

where T_i is the state progression time of S_i defined by

$$T_i:=\inf\left\{t\in\mathbb{R}^+:M(t)=i\right\}. \quad (6)$$

Random walk S_i is a stationary Markov chain starting from $S_0=0$. The state transition probabilities from S_{i-1} to S_i equals the probabilities that a point arrival of $M(t)$ comes

from either $H(t)$ or $A(t)$. Specifically, the state transition probabilities are written as

$$p_A := \Pr(S_i = n+1 | S_{i-1} = n) = \frac{\lambda_A}{\lambda_T}, \quad (7)$$

and

$$p_H := \Pr(S_i = n-1 | S_{i-1} = n) = \frac{\lambda_H}{\lambda_T}, \quad (8)$$

for all $i \in \mathbb{Z}^+$ and $n \in \mathbb{Z}$. The state transition probabilities p_H and p_A are the proportions of computing power occupied by the normal miners and that by the attacker, respectively.

We define the independent and identically distributed (i.i.d.) state transition random variables $\Delta_i \in \{\pm 1\} \sim \text{Bernoulli}(p_H)$ as

$$\Delta_i := S_i - S_{i-1}, \quad (9)$$

for $i \in \mathbb{Z}^+$.

Using the random walk, we can rewrite $T^{(1),(2)}$ as

$$T^{(1),(2)} = \min\left\{\left\{T_i : H(T_i) \geq N_{BC}; S_i < 0, \forall i \in \mathbb{Z}^+\right\} \cup \{\infty\}\right\}. \quad (10)$$

C. Event sets of random walk

We aim to construct the event sets of state transitions Δ_i which imply the satisfaction of the two conditions in (10): $H(T_i) \geq N_{BC}$ (i.e., $\mathcal{G}^{(1)}$) and $S_i < 0$ (i.e., $\mathcal{G}^{(2)}$).

For the purpose, we define a DS attack as random experiment $\mathbf{\Delta}_I = \mathcal{A}(p_A, t_{cut}; N_{BC})$ which produces random binary sequence $\mathbf{\Delta}_I := (\Delta_1, \cdots, \Delta_i) \in \{\pm 1\}^I$ of the state transitions in (9) with random length $I \in \mathbb{Z}^+$. The experimental output is an element of universal set $\mathcal{U}$ of sequences, which is defined as

$$\mathcal{U} := \bigcup_{i=1}^{\infty} \mathcal{U}_i = \bigcup_{i=1}^{\infty} \{\pm 1\}^i, \quad (10)$$

where $\mathcal{U}_i := \{\pm 1\}^i$. We define $\boldsymbol{\delta}_i := (\delta_1, \cdots, \delta_i) \in \mathcal{U}_i$ as a binary sequence of length i, which is the realization of $\mathbf{\Delta}_I$. We denote $s_k := \sum_{l=1}^{k} \delta_l$ for integer $k \in \mathbb{Z}^+$, which comprises observations of the state variables S_k of the random walk.

We denote the event sets $\mathcal{W}_i \subset \mathcal{U}_i$, for $i \in \mathbb{Z}^+$, each of which satisfies $\mathcal{G}^{(1)}$ and $\mathcal{G}^{(2)}$ at the *i*-th state for the first time. The time $T^{(1),(2)}$ in (10) then can be rewritten as

$$T^{(1),(2)} = \min\left\{\left\{T_i : \mathbf{\Delta}_I \in \mathcal{W}_i, \forall i \in \mathbb{Z}^+\right\} \cup \{\infty\}\right\}. \quad (11)$$

To construct $\mathcal{W}_i$, we divide it into mutually exclusive sets $\mathcal{D}_j^{(1)}$ and $\mathcal{D}_{j,i}^{(2)-(1)}$, for $j = 1, \cdots, i$.

Set $\mathcal{D}_j^{(1)}$ is a subset of $\mathcal{U}_i$ such that $\mathcal{G}^{(1)}$ is satisfied exactly at the j-th state S_j. One of the requirements on the binary sequences of $\mathcal{D}_j^{(1)}$ is $s_j = 2N_{BC} - j$ since the first j transitions δ_k for $k = 1, \cdots, j$ have N_{BC} number of $+1$'s and $j - N_{BC}$ number of -1's.

Set $\mathcal{D}_{j,i}^{(2)-(1)}$ for $j \leq i$ is a subset of $\mathcal{U}_i$ such that $\mathcal{G}^{(2)}$ is satisfied for the first time at the i-th state and $\mathcal{G}^{(1)}$ is satisfied already at state j prior or equal to state i. This set does not care about the first j transitions δ_k for $k = 1, \cdots, j$, but only focuses on the interim transitions from the $j+1$-th to the i-th, i.e. δ_m, for $m = j+1, \cdots, i$. Recall that satisfying $\mathcal{G}^{(1)}$ at state j implies $s_j = 2N_{BC} - j$. Thus, the requirement for the elements of $\mathcal{D}_{j,i}^{(2)-(1)}$ is that the state changes from starting state $s_j = 2N_{BC} - j$ to state $s_i = -1$, while any interim state s_k remains non-negative; i.e., $s_k \geq 0$ for each $k = j+1, \cdots, i-1$.

The elements of joint set $\mathcal{D}_j^{(1)} \bigcap \mathcal{D}_{j,i}^{(2)-(1)}$ for $j \leq i$ satisfy both $\mathcal{G}^{(1)}$ at state j and $\mathcal{G}^{(2)}$ at state i. When $j > i$, the elements of $\mathcal{D}_j^{(1)} \bigcap \mathcal{D}_{j,i}^{(2)-(1)}$ does not imply achieving $\mathcal{G}^{(1)}$ and $\mathcal{G}^{(2)}$ at the i-th state, since no confirmation has been obtained yet. Namely, achieving $\mathcal{G}^{(1)}$ and $\mathcal{G}^{(2)}$ is possible at a state only posterior to the state at which $\mathcal{G}^{(1)}$ is satisfied. When $j < N_{BC}$, $\mathcal{D}_j^{(1)} = \phi$ due to an insufficient number of state transitions for the block confirmation. Subsequently, $\mathcal{W}_i$ is written as

$$\mathcal{W}_i = \bigcup_{j=N_{BC}}^{i} \mathcal{D}_j^{(1)} \bigcap \mathcal{D}_{j,i}^{(2)-(1)}. \quad (12)$$

We further explore (12). Remember that in the first j transitions of $\mathcal{D}_j^{(1)}$, the number of $+1$'s is fixed to N_{BC} and the rests of $j - N_{BC}$ transitions are -1's. This implies that for $j > 2N_{BC}$, s_j in $\mathcal{D}_j^{(1)}$ are already negative. Equivalently, for $j > 2N_{BC}$, elements in $\mathcal{D}_j^{(1)}$ satisfy both $\mathcal{G}^{(1)}$ and $\mathcal{G}^{(2)}$ at state j. Analogously, $\mathcal{D}_{j,i}^{(2)-(1)} = \phi$ for $j > 2N_{BC}$ and $j < i$, since the state $s_j = 2N_{BC} - j$ contradicts the requirement of $\mathcal{D}_{j,i}^{(2)-(1)}$: the interim transactions between s_j and s_i should be non-negative. For $j > 2N_{BC}$ and $j = i$, set $\mathcal{D}_{j,i}^{(2)-(1)}$ about interim states s_k, for $k = j+1, \cdots, i-1$, equals set $\mathcal{U}_i$ since there is no interim state to apply the requirement to. This implies $\mathcal{D}_j^{(1)} \bigcap \left(\mathcal{D}_{j,i}^{(2)-(1)}\right) = \mathcal{D}_i^{(1)}$ for $j > 2N_{BC}$ and $j = i$.

As a result, (12) becomes

$$\mathcal{W}_i = \begin{cases} \left(\bigcup_{j=N_{BC}}^{2N_{BC}} \mathcal{D}_j^{(1)} \bigcap \mathcal{D}_{j,i}^{(2)-(1)} \right) \cup \mathcal{D}_i^{(1)}, & \text{for } i > 2N_{BC}, \\ \phi, & \text{for } i \leq 2N_{BC}. \end{cases} \quad (13)$$

For example, suppose $N_{BC}=2$, then a sequence $\boldsymbol{\Delta}_5=(-1,+1,+1,-1,-1)$ satisfies $\mathcal{G}^{(1)}$ at state index $j=3$. After the 3-rd index, $\boldsymbol{\Delta}_5$ satisfies $\mathcal{G}^{(2)}$ at $i=5$, thus $\boldsymbol{\Delta}_5\in\left(\mathcal{D}_3^{(1)}\bigcap\mathcal{D}_{3,5}^{(2)\text{–}(1)}\right)\subset\mathcal{W}_5$. The other example is a sequence $\boldsymbol{\Delta}_5=(-1,-1,+1,-1,+1)$, which satisfies $\mathcal{G}^{(1)}$ at $j=5$ for the first time. In addition, at the same state index, the sequence $\boldsymbol{\Delta}_5$ satisfies $\mathcal{G}^{(2)}$ as well. Hence, $\boldsymbol{\Delta}_5\in\mathcal{D}_5^{(1)}\subset\mathcal{W}_5$. It is easy to check that for all $j>2N_{BC}$, the sequences which satisfy $\mathcal{G}^{(1)}$ at the j-th state index for the first time satisfy $\mathcal{G}^{(2)}$ as well at the same state index, and thus are the elements of $\mathcal{W}_i$. As a counterexample, a sequence $\boldsymbol{\Delta}_4=(-1,-1,+1,+1)$ satisfies $\mathcal{G}^{(1)}$ at the 4-th state index, but never satisfies $\mathcal{G}^{(2)}$ due to the number of state transitions being insufficient.

The sets $\mathcal{W}_i$ for $i\in\mathbb{Z}^+$ are mutually exclusive since the lengths of the sequences comprising these differ by i. Thus, for DS attack $\boldsymbol{\Delta}_I=\mathcal{A}(p_A,t_{cut};N_{BC})$, if i exists such that $\boldsymbol{\Delta}_I\in\mathcal{W}_i$, for $i\in\mathbb{Z}^+$, then it is unique, which implies that the expression for $T^{(1),(2)}$ in (11) can be rewritten as

$$T^{(1),(2)}=\begin{cases}T_i, & \text{if } \exists i\text{: } \boldsymbol{\Delta}_I\in\mathcal{W}_i,\ \forall i\in\mathbb{Z}^+,\\ \infty, & \text{otherwise.}\end{cases} \tag{14}$$

III. AS Probabilities

For a DS attack task $\boldsymbol{\Delta}_I=\mathcal{A}(p_A,t_{cut};N_{BC})$, we aim to compute the probability of AS, which equals the probability that the AS conditions $\mathcal{G}^{(1)}$ and $\mathcal{G}^{(2)}$ have met within the time duration t_{cut}; i.e., $T^{(1),(2)}<t_{cut}$. This probability requires the probability density function (PDF) of $T^{(1),(2)}$, which also enables to compute the expectation of the time at which a DS attack succeeds, i.e., expected AS time.

The probabilities and expectations in this section will be used to evaluate the profitability of DS attacks in Section IV.

A. AS-ICT Probability

We first compute the probability of AS-ICT with $t_{cut}=\infty$. The probability of AS-ICT is the probability that the state index i exists such that $\boldsymbol{\Delta}_I\in\mathcal{W}_i$, and thus requires $\Pr(\boldsymbol{\Delta}_I\in\mathcal{W}_i)$. Note that no occurrence of AS-ICT with infinite t_{cut} implies no occurrence of AS with a finite t_{cut} as well. That is to say, the probability of AS-ICT is also needed to compute the probability of AS.

In specific, from the mutual exclusiveness of $\mathcal{W}_i$ for $i\in\mathbb{Z}^+$, the probability $\mathbb{P}_{AS-ICT}$ of AS-ICT equals the sum of $\Pr(\boldsymbol{\Delta}_I\in\mathcal{W}_i)$, for $i\in\mathbb{Z}^+$. Since $\mathcal{W}_i=\phi$, for $i\le 2N_{BC}$, as given in (13), it can be computed as

$$\mathbb{P}_{AS-ICT}(p_A;N_{BC})=\sum_{i=2N_{BC}+1}^{\infty}\Pr(\boldsymbol{\Delta}_I\in\mathcal{W}_i). \tag{15}$$

The following Proposition 2 gives the probability $\Pr(\boldsymbol{\Delta}_I\in\mathcal{W}_i)$ used in (15).

Proposition 2. *Consider DS attack task $\boldsymbol{\Delta}_I=\mathcal{A}(p_A,t_{cut};N_{BC})$, then the probability that $\Pr(\boldsymbol{\Delta}_I\in\mathcal{W}_i)$, for $i>2N_{BC}$, can be computed as*

$$\begin{aligned}\Pr(\boldsymbol{\Delta}_I\in\mathcal{W}_i)&=\sum_{j=N_{BC}}^{j=2N_{BC}}\binom{j-1}{N_{BC}-1}C_{\frac{i-1}{2}-N_{BC},2N_{BC}-j}\,p_A^{\frac{i+1}{2}}p_H^{\frac{i-1}{2}}\\&\quad+\binom{i-1}{N_{BC}-1}p_H^{N_{BC}}p_A^{i-N_{BC}},\end{aligned} \tag{16}$$

where

$$C_{n,m}=\begin{cases}\dfrac{m+1}{n+m+1}\dbinom{2n+m}{n}, & n,m\in\mathbb{Z}^+\bigcup\{0\},\\ 0, & \text{otherwise,}\end{cases} \tag{17}$$

and for $i\le 2N_{BC}$, $\Pr(\boldsymbol{\Delta}_I\in\mathcal{W}_i)=0$.

Proof: As given in (13), set $\mathcal{W}_i$ is the union of $\mathcal{D}_j^{(1)}\bigcap\mathcal{D}_{j,i}^{(2)\text{–}(1)}$, for $j=N_{BC},\cdots,2N_{BC}$ and $\mathcal{D}_i^{(1)}$. As sets $\mathcal{D}_j^{(1)}$, for $j=N_{BC},\cdots,2N_{BC}$, are mutually exclusive by definition, the probability of the union of $\mathcal{D}_j^{(1)}\bigcap\mathcal{D}_{j,i}^{(2)\text{–}(1)}$, for $j=N_{BC},\cdots,2N_{BC}$, and $\mathcal{D}_i^{(1)}$ equals the sum of the respective probabilities. In addition, for every $i\ge 2N_{BC}+1$ and j, $\mathcal{D}_j^{(1)}$ and $\mathcal{D}_{j,i}^{(2)\text{–}(1)}$ are independent since the requirements for the two sets focus on the different indices of the state transitions. Thus, the probability of intersections $\mathcal{D}_j^{(1)}\bigcap\mathcal{D}_{j,i}^{(2)\text{–}(1)}$ equals the product of the respective probabilities. As a result, from (13), $\Pr(\boldsymbol{\Delta}_I\in\mathcal{W}_i)$ for $i>2N_{BC}$ can be computed as

$$\begin{aligned}\Pr(\boldsymbol{\Delta}_I\in\mathcal{W}_i)=&\sum_{j=N_{BC}}^{j=2N_{BC}}\Pr(\boldsymbol{\Delta}_I\in\mathcal{D}_j^{(1)})\Pr(\boldsymbol{\Delta}_I\in\mathcal{D}_{j,i}^{(2)\text{–}(1)})\\&+\Pr(\boldsymbol{\Delta}_I\in\mathcal{D}_i^{(1)}).\end{aligned} \tag{18}$$

By definition, set $\mathcal{D}_j^{(1)}$ picks $N_{BC}-1$ transitions among the first $j-1$ transitions. The picked transitions are given $+1$ s and the rests are given -1 s. The j-th transition is $\Delta_j=1$. The probability $\Pr(\mathcal{D}_j^{(1)})$ equals the point mass function of a negative binomial distribution:

$$\Pr(\mathcal{D}_j^{(1)})=\binom{j-1}{N_{BC}-1}p_H^{N_{BC}}p_A^{j-N_{BC}}. \tag{19}$$

Computing the probability $\Pr(\mathcal{D}_{j,i}^{(2)\text{–}(1)})$ starts from counting the number of elements in $\mathcal{D}_{j,i}^{(2)\text{–}(1)}$. Remember the requirements on every element of $\mathcal{D}_{j,i}^{(2)\text{–}(1)}$, for $j=N_{BC},\cdots,2N_{BC}$, are that the states change starting from state $s_j=2N_{BC}-j$ and ending with state $s_i<0$ while keeping $s_k\ge 0$, for $k=j+1,\cdots,i-1$. The i-th transition should be $\Delta_i=-1$. The number of elements in $\mathcal{D}_{j,i}^{(2)\text{–}(1)}$ equals the ballot number [21], which is the number of random walks that consist of $i-j-1$ steps and never become negative,

starting from point $2N_{BC}-j$ at the j-th state and ending at the origin with the $i-1$-th state. This number is given as $C_{n,m}$ in (17) with relationships $2n+m=i-j-1$ and $m=2N_{BC}-j$. As a result, by multiplying the probabilities of state transitions, the probability $\Pr\left(\mathcal{D}_{j,i}^{(2)\text{-}(1)}\right)$ is computed as

$$\Pr\left(\mathcal{D}_{j,i}^{(2)\text{-}(1)}\right)=C_{n,m}{p_A}^{(n+m+1)}{p_H}^{n}. \tag{20}$$

Finally, substituting (19) and (20) into (18) results in (16). ■

The following Corollary 3 gives an explicit formula of the probability $\mathbb{P}_{AS-ICT}$ of AS-ICT given in (15).

Corollary 3. *The probability $\mathbb{P}_{AS-ICT}$ has an algebraic expression*

$$\mathbb{P}_{AS-ICT}\left(p_A;N_{BC}\right)=\begin{cases}1, & p_H\le p_A,\\ 1-{p_A}^{N_{BC}+1}{p_H}^{N_{BC}}\displaystyle\sum_{j=N_{BC}}^{2N_{BC}}\binom{j-1}{N_{BC}-1}A_j, & p_H>p_A,\end{cases} \tag{21}$$

where

$$A_j\triangleq{p_A}^{j-2N_{BC}-1}-{p_H}^{j-2N_{BC}-1}. \tag{22}$$

Proof: See Appendix A

B. AS Probability

By Definition 1, the probability of AS equals

$$\mathbb{P}_{AS}\left(p_A,t_{cut};N_{BC}\right):=\Pr\left(T^{(1),(2)}<t_{cut}\right). \tag{23}$$

To compute $\mathbb{P}_{AS}$, we need the probability density function (PDF) of $T^{(1),(2)}$. From the mutual exclusiveness of $\mathcal{W}_i$ for integers $i>2N_{BC}$ and the relationship in (14), the PDF $f_{T^{(1),(2)}}$ can be computed as

$$\begin{aligned}f_{T^{(1),(2)}}(t)=&\sum_{i=2N_{BC}+1}^{\infty}\Pr\left(\mathbf{\Delta}_I\in\mathcal{W}_i\right)f_{T_i}(t)\\&+\left(1-\mathbb{P}_{AS-ICT}\right)\delta\left(t-\infty\right),\end{aligned} \tag{24}$$

where $\delta(t)$ is a Dirac delta function and $f_{T_i}(t)$ is the PDF of T_i. The random variable T_i in (6) follows an Erlang distribution with shape parameter i and rate λ_T [20]. The PDF of T_i is thus given as

$$f_{T_i}(t)=\frac{\lambda_T\left(\lambda_T t\right)^{i-1}e^{-\lambda_T t}}{(i-1)!}. \tag{25}$$

Proposition 4. *The PDF of time $T^{(1),(2)}$ has a closed-form expression:*

$$\begin{aligned}f_{T^{(1),(2)}}(t)=&\frac{p_A\lambda_T e^{-\lambda_T t}\left(p_A p_H\left(\lambda_T t\right)^2\right)^{N_{BC}}}{(2N_{BC})!}\\&\cdot\sum_{j=N_{BC}}^{j=2N_{BC}}\binom{j-1}{N_{BC}-1}{}_2F_3\left(\mathbf{a};\mathbf{b};p_A p_H\left(\lambda_T t\right)^2\right)\\&+\frac{e^{-\lambda_T t}}{t}\frac{\left(p_H\lambda_T t\right)^{N_{BC}}}{(N_{BC}-1)!}\left(e^{p_A\lambda_T t}-\sum_{i=0}^{N_{BC}}\frac{\left(p_A\lambda_T t\right)^i}{i!}\right)\\&+\left(1-\mathbb{P}_{AS-ICT}\right)\delta\left(t-\infty\right),\end{aligned} \tag{26}$$

where ${}_pF_q\left(\mathbf{a};\mathbf{b};x\right)$ is the generalized hypergeometric function [22] defined in Appendix E with the parameter vectors

$$\mathbf{a}=\begin{bmatrix}N_{BC}+1-j/2\\ N_{BC}+1/2-j/2\end{bmatrix} \tag{27}$$

and

$$\mathbf{b}=\begin{bmatrix}2N_{BC}+2-j\\ N_{BC}+1\\ N_{BC}+1/2\end{bmatrix}. \tag{28}$$

Proof: See Appendix B.

C. Expected AS Times

It will be shown to be convenient to define the AS time as

$$T_{AS}:=\begin{cases}T^{(1),(2)}, & \text{if } T^{(1),(2)}<t_{cut},\\ \text{not defined}, & \text{otherwise.}\end{cases} \tag{29}$$

The case for $T_{AS}>t_{cut}$ does not need to be defined since it is not useful.

The PDF of T_{AS} is just a scaled version of $f_{T^{(1),(2)}}(t)$ for $0<t<t_{cut}$, which is given in (26), with a scaling factor of $\mathbb{P}_{AS}^{-1}$. Formally, the PDF $f_{T_{AS}}(t)$ equals

$$f_{T_{AS}}(t)=\begin{cases}\dfrac{f_{T^{(1),(2)}}(t)}{\mathbb{P}_{AS}\left(p_A,t_{cut};N_{BC}\right)}, & \text{for } 0\le t<t_{cut},\\ 0, & \text{for } t\ge t_{cut}.\end{cases} \tag{30}$$

The expectation of AS time (EAST) is computed as

$$\mathbb{E}_{T_{AS}}\left(p_A,t_{cut};N_{BC}\right)=\frac{\int_0^{t_{cut}}tf_{T^{(1),(2)}}(t)\,dt}{\mathbb{P}_{AS}\left(p_A,t_{cut};N_{BC}\right)}. \tag{31}$$

Similarly, we define AS-ICT time as the AS time with $t_{cut}=\infty$. From the results (24) and (31), if $t_{cut}=\infty$, the expectation of the time for AS-ICT is computed as follow

$$\mathbb{E}_{T_{AS-ICT}}\left(p_A;N_{BC}\right)=\frac{\lim_{t_{cut}\to\infty^-}\int_0^{t_{cut}} t f_{T^{(1),(2)}}(t)\,dt}{\mathbb{P}_{AS-ICT}\left(p_A;N_{BC}\right)}$$
$$=\frac{\sum_{i=2N_{BC}+1}^{\infty}\mathbb{E}[T_i]\Pr\left(\boldsymbol{\Delta}_I\in\mathcal{W}_i\right)}{\mathbb{P}_{AS-ICT}\left(p_A;N_{BC}\right)} \quad (32)$$
$$=\frac{\sum_{i=2N_{BC}+1}^{\infty}\frac{i}{\lambda_T}\Pr\left(\boldsymbol{\Delta}_I\in\mathcal{W}_i\right)}{\mathbb{P}_{AS-ICT}\left(p_A;N_{BC}\right)},$$

where $E[T_i]=i\lambda_T^{-1}$ [20].

The following Proposition 5 gives an explicit formula of $\mathbb{E}_{T_{AS-ICT}}$.

Proposition 5. *Let* $p_M:=\max(p_A,p_H)$ *and* $p_m:=\min(p_A,p_H)$, *then the expectation* $\mathbb{E}_{T_{AS-ICT}}$ *has a closed-form expression:*

$$\mathbb{E}_{T_{AS-ICT}}\left(p_A;N_{BC}\right)=\frac{\lambda_T^{-1}\left(\sum_{j=N_{BC}}^{2N_{BC}}\binom{j-1}{N_{BC}-1}Z_j+\frac{N_{BC}}{p_H}\right)}{\mathbb{P}_{AS-ICT}\left(p_A;N_{BC}\right)}, \quad (33)$$

where

$$Z_j:=p_A p_m^{N_{BC}}p_M^{-(N_{BC}-j+1)}\left(\frac{2N_{BC}-2jp_m+1}{p_M-p_m}\right)$$
$$-jp_A^{-(N_{BC}-j)}p_H^{N_{BC}}. \quad (34)$$

Proof: See Appendix A.

D. Comparison with Previous Works

The AS-ICT probability $\mathbb{P}_{AS-ICT}$ (AS probability when indefinite cut time $t_{cut}=\infty$ is given) in Corollary 3 was computed by Nakamoto [1] and Rosenfield [15] using the gambler's ruin theorem [23]. In [1], Nakamoto suggested an additional assumption not in our scenario: the time spent for the first N_{BC} blocks mined by the normal group is not random and is determined as the average time $\lambda_H^{-1}N_{BC}$ instead. In other words, the block confirmation process was not treated as the stochastic processes. In [15], Rosenfield removed the assumption proposed by Nakamoto to derive the result in Corollary 3. However, the result was still based on the gambler's ruin theorem which only computes the asymptotical behavior of S_n as $n\to\infty$ by manipulating the recurrence relationship between two adjacent states. That is to say, he assumed that an indefinite number of attack chances are given to the attacker. There was no result related to the intermediate process such as Proposition 2.

In this paper, we introduce t_{cut}, which generalize the results by Nakamoto and Rosenfield, and compute the AS probability $\mathbb{P}_{AS}$ using Proposition 2. In practice, attack chances are limited since the amount of resources such as time and cost are limited, and therefore a cut time t_{cut} is needed to cut loss.

Besides the probability $\mathbb{P}_{T_{AS-ICT}}$, the probability distribution of attack success time similar with $T^{(1),(2)}$ was also analyzed in [16], [18], and [19]. However, none of the results matched with the AS conditions in Definition 1.

In [18], Goffard considered the race between two PCPs $H(t)$ and $A(t)$ with unfair initial states. Specifically, the initial states of the public chain $H(t)$ and the fraudulent chain were set to $H(0)=z$ and $A(0)=0$ for integer $z>0$, respectively, then an implicit expression of the probability distribution of first time τ_z at which $H(\tau_z)=A(\tau_z)$ was analyzed. Time τ_z can be interpreted as the interval spent for $\mathcal{D}_{j,i}^{(2)-(1)}$; i.e., the interval from the time at which $\mathcal{G}^{(1)}$ alone is satisfied to the time at which both $\mathcal{G}^{(1)}$ and $\mathcal{G}^{(2)}$ are satisfied. This analysis did not consider the time for $\mathcal{G}^{(1)}$.

In [16], Bissias *et al.* also considered the race between two PCPs. To derive an explicit formula of the probability distribution of AS time, they put in other conditions to end an attack attempt: the attack stops if either $H(t)$ or $A(t)$ reaches $N_{BC}+1$, whichever happens first. In other words, the only way to succeed in an attack is that the fraudulent chain should mine $N_{BC}+1$ blocks faster than the public chain. On the contrary, in our model and in reality, an attack can be continued even at a moment when the public chain is ahead of the fraudulent chain, if it will give any profit.

In [19], Karame *et al.* analyzed the first AS time under a fast-payment model which removed the block confirmation process by omitting condition $\mathcal{G}^{(1)}$.

IV. The Expected Profit of a DS Attack

The previous probabilistic analyses in [1] and [15] show that the success of DS attacks is not guaranteed when $p_A<0.5$. However, DS attacks with $p_A<0.5$ might be pursued if they bring profit.

A. Profitable DS Attacks

Here, we analyze the *profitability* of DS attacks and to this end, we define profit function P of DS attack $\mathcal{A}(C,p_A,t_{cut};N_{BC})$ in terms of value C of a fraudulent transaction, the block mining reward, and the operating expense (OPEX) of the computing power. We compute the expected profit function $\mathbb{E}_P(p_A,t_{cut};N_{BC})$, which is the expectation of P.

Definition 6 (Profitable Attacks). *DS attack* $\mathcal{A}(C,p_A,t_{cut};N_{BC})$ *is said to be profitable if and only if* $\mathbb{E}_P>0$.

The OPEX (e.g. the rental fee for the computing power) and the block mining reward are increased by the average block mining speed λ_A by the attacker and the time t consumed during an attack. Thus, the OPEX and block mining rewards are expressed as functions $X(\lambda_A,t)$ and $R(\lambda_A,t)$, respectively, which can be any increasing function (e.g., linear, exponential, or log) with respect to λ_A and t. We define X and R, respectively, as follows:

$$X(\lambda_A,t):=\gamma\lambda_A t\left(\log_{x_1}x_2\right)^{\lambda_A}\left(\log_{x_3}x_4\right)^t \quad (35)$$

for real constants $\gamma > 0$, $x_1, x_2 > 1$, and $x_3, x_4 > 1$, and

$$R(\lambda_A, t) := \beta \lambda_A t \left(\log_{r_1} r_2\right)^{\lambda_A} \left(\log_{r_3} r_4\right)^t \tag{36}$$

for real constants β, $r_1, r_2 > 1$, and $r_3, r_4 > 1$.

To sum up, if an attack succeeds, the income from the AS is C as it is double-spent and the block mining reward R for time duration T_{AS}. In this case, the cost is the OPEX for duration T_{AS}. If the attack fails, the cost is the OPEX for duration t_{cut} without revenue. Hence, profit P of a DS attack is the random variable

$$P := \begin{cases} C + R(\lambda_A, T_{AS}) - X(\lambda_A, T_{AS}), & \text{if } T^{(1),(2)} < t_{cut}, \\ -X(\lambda_A, t_{cut}), & \text{otherwise.} \end{cases} \tag{37}$$

Subsequently, the expected profit function of a DS attack is

$$\begin{aligned} &\mathbb{E}_P(p_A, t_{cut}; N_{BC}) = \\ &\quad \mathbb{P}_{AS}(p_A, t_{cut}; N_{BC})\left(C + \mathbb{E}\left[R(\lambda_A, T_{AS})\right] - \mathbb{E}\left[X(\lambda_A, T_{AS})\right]\right) \\ &\quad -\left(1 - \mathbb{P}_{AS}(p_A, t_{cut}; N_{BC})\right) X(\lambda_A, t_{cut}) \\ &= \mathbb{P}_{AS}(p_A, t_{cut}; N_{BC})\left(C + \mathbb{E}\left[R(\lambda_A, T_{AS})\right]\right) - \mathbb{E}_X(p_A, t_{cut}; N_{BC}), \end{aligned} \tag{38}$$

where $\lambda_A = p_A \lambda_T$ and $\mathbb{E}_X$ is the expected OPEX defined as

$$\begin{aligned} &\mathbb{E}_X(p_A, t_{cut}; N_{BC}) := \\ &\quad \mathbb{P}_{AS}(p_A, t_{cut}; N_{BC}) \mathbb{E}\left[X(\lambda_A, T_{AS})\right] \\ &\quad + \left(1 - \mathbb{P}_{AS}(p_A, t_{cut}; N_{BC})\right) X(\lambda_A, t_{cut}). \end{aligned} \tag{39}$$

Definition 6 and (38) imply that for fixed p_A and t_{cut}, DS attack $\mathcal{A}(C, p_A, t_{cut}; N_{BC})$ is profitable if and only if $C > C_{\text{Req.}}$, where the required value of target transaction $C_{\text{Req.}}$ is

$$C_{\text{Req.}} = \frac{\mathbb{E}_X(p_A, t_{cut}; N_{BC})}{\mathbb{P}_{AS}(p_A, t_{cut}; N_{BC})} - \mathbb{E}\left[R(\lambda_A, T_{AS})\right]. \tag{40}$$

Theorem 7. *Suppose $x_1 = x_2$ and $x_3 = x_4$ in (35), and $r_1 = r_2$ and $r_3 = r_4$ in (36). DS attack $\mathcal{A}(C, p_A, t_{cut}; N_{BC})$ for $p_A \in (0, 0.5)$ is profitable only if $t_{cut} < \infty$. In addition, let $t_{cut} = \infty$ and $p_A \in (0.5, 1)$, then the required value of target transaction in* (40) *becomes*

$$C_{\text{Req.}} = \max\left(0, (\gamma - \beta) \lambda_T p_A \mathbb{E}_{T_{AS-ICT}}(p_A; N_{BC})\right). \tag{41}$$

Proof: See Appendix C.

By Theorem 7, setting $t_{cut} = \infty$ and $p_A \in (0, 0.5)$ makes DS attack non-profitable. The following Theorem 8 shows that by setting a finite t_{cut}, DS attacks $\mathcal{A}(C, p_A, t_{cut}; N_{BC})$ can be profitable not only for $p_A \in (0.5, 1)$, but also for $p_A \in (0, 0.5)$.

Theorem 8. *Let $x_1 = x_2$ and $x_3 = x_4$ in (35), and $r_1 = r_2$ and $r_3 = r_4$ in (36). Let $t_{cut} = c\mathbb{E}_{T_{AS-ICT}}(p_A; N_{BC})$ for a positive real c, where $\mathbb{E}_{T_{AS-ICT}}$ is given in* (33). *A DS attack $\mathcal{A}(C, p_A, t_{cut}; N_{BC})$ is profitable for any $p_A \in (0, 1)$, if $C > C_{\text{Suf.}}$, where*

$$C_{\text{Suf.}} = \gamma'(p_A, c) \frac{\lambda_T p_A \mathbb{E}_{T_{AS-ICT}}(p_A; N_{BC})}{\mathbb{P}_{AS}(p_A, t_{cut}; N_{BC})}, \tag{42}$$

and

$$\gamma'(p_A, c) := \gamma \cdot \left(\frac{\mathbb{P}_{AS-ICT}(p_A; N_{BC})}{\mathbb{P}_{AS}(p_A, t_{cut}; N_{BC})} + c\left(1 - \mathbb{P}_{AS}(p_A, t_{cut}; N_{BC})\right) \right). \tag{43}$$

Proof: See Appendix D.

B. Profitable DS Attacks against Working Blockchain Networks

As of 9th December 2018, we refer to blockchain explorers and *nicehash.com* (who provides the rental rates for borrowing computing power) to obtain block mining reward R and OPEX X. The parameters $x_1, \cdots, x_4$ used in (35) are set to $x_1 = x_2$ and $x_3 = x_4$, which leads to a linear function

TABLE I
NUMERICAL COMPUTATIONS OF REQUIRED RESOURCES FOR PROFITABLE DS ATTACKS WHEN $t_{cut} = c\mathbb{E}_{T_{AS-ICT}}$, FOR $c=2$.

Block Confirmation Number (N_{BC})		1		3		5		7		9	
Computing Power (p_A)		0.35	0.4	0.35	0.4	0.35	0.4	0.35	0.4	0.35	0.4
Cut Time (t_{cut})	Scaled by λ_H^{-1}	7.593	9.491	13.548	15.617	19.217	21.294	24.753	26.755	30.212	32.084
AS Probability ($\mathbb{P}_{AS}$)		0.389	0.523	0.286	0.440	0.217	0.380	0.167	0.332	0.130	0.292
Expected AS Time ($\mathbb{E}_{T_{AS}}$)	Scaled by λ_H^{-1}	2.640	2.801	5.682	5.732	8.621	8.553	11.498	11.316	14.333	14.039
Expected OPEX ($\mathbb{E}_X$)	Scaled by γ	3.050	3.993	6.085	7.513	9.110	10.973	12.135	14.423	15.153	17.874
Required Value of Target Transaction ($C_{\text{Suf.}}$)		12.257	12.535	31.967	26.253	62.545	43.457	107.812	64.728	172.757	90.660

X with respect to λ_A and T_{AS}. Analogously, the parameters for R in (36) are set to $r_1 = r_2$ and $r_3 = r_4$, leading to a linear function R with respect to λ_A and T_{AS}. There are three more parameters: γ, β, and λ_H^{-1}. Parameter γ is the expected cost spent per generating a block and required for computing the expected OPEX. Parameter β is the reward per generating a block. Parameter λ_H^{-1} is the average block generation time of the public chain. They are different by blockchain networks.

We consider the *Syscoin* and *BitcoinCash* networks. The parameter γ is obtainable from *nicehash.com.* The two networks use the *SHA-256* cryptographic puzzle for which the unit of computation is *hash.* The rental fee for 1P hashes per second for a day is around 0.04 BTC, which is around $4.63 \cdot 10^{-7}$ BTC per second. In other words, the rental fee is approximately $4.63 \cdot 10^{-22}$ BTC per the computing of a hash.

Once parameters β, γ, and λ_H^{-1} are obtained, the required attack resources can be evaluated using Table I. Table I lists the required attack resources for each $p_A = 0.35$ and $p_A = 0.4$ when $t_{cut} = c\mathbb{E}_{T_{AS-ICT}}$, for $c = 2$.

1) The Syscoin Network Parameters

The average block generation time is fixed at $\lambda_H^{-1} = 60$ seconds. Referring to *poolexplorer.com*, the network's computing speed is 7.6E hashes per second; i.e., 7.6E·60=456E solutions are needed to mine one block on average. Then, the parameter γ is obtained as

$$\begin{aligned}\gamma &= 4.63 \cdot 10^{-22}\ [\text{BTC/hash}] \\ &\quad \times 456\text{E}[\text{hashes/block mining}] \\ &\approx 0.21\ [\text{BTC/block mining}].\end{aligned} \tag{44}$$

The reward β per block mining is 38.5 SYS (without transaction fees), which is around $3.6 \cdot 10^{-4}$ BTC per block mining.

2) The BitcoinCash Network Parameters

The average block generation time is fixed at $\lambda_H^{-1} = 600$ seconds. Referring to *BTC.com*, the network's computing speed is 1.2E hashes per second; i.e., 1.2E·600=720E hashes are needed to generate one block on average. The parameter γ is obtained as

$$\begin{aligned}\gamma &= 4.63 \cdot 10^{-22}\ [\text{BTC/hash}] \\ &\quad \times 720\text{E}[\text{hashes/block mining}] \\ &\approx 0.33\ [\text{BTC/block mining}].\end{aligned} \tag{45}$$

Table II
EVALUATION OF RESOURCES REQUIRED FOR PROFITABLE ATTACK AGAINST WORKING BLOCKCHAIN NETOWKRS ($p_A = 0.35$, $N_{BC} = 5$).

Target Network	*Syscoin*	*BitcoinCash*
Cut Time (Seconds)	1153	11530
Required Value of Target Transaction (BTC)	13.134	20.639
Expected OPEX (BTC)	1.810	2.844
Expected AS Time (Seconds)	546	5466

The reward β per block mining is 12.5 BCH (without transaction fees), which is around 0.57 BTC per block mining. By Theorem 7, the relationship $\beta > \gamma$ implies that the required value $C_{\text{Req.}} = 0$ for DS attack $\mathcal{A}(C, p_A, t_{cut}; N_{BC})$ with $p_A > 0.5$ and $t_{cut} = \infty$ to be profitable is 0; i.e., such DS attacks are always profitable regardless of the value C of target transaction.

3) DS Attack with a Finite Cut Time and $p_A < 0.5$

In Table II, we evaluate the resources required for profitable DS attacks using $p_A = 0.35$ against the two blockchain networks. The values in Table II are obtained from the values in Table I multiplied by scaling parameters γ and λ_H^{-1}. The results explain the importance of network parameter λ_H^{-1}. Remember that *Syscoin* has a greater network computing power (7.6E hashes per second) than *BitcoinCash* (1.2E hashes per second). This implies that *Syscoin* has a higher rental fee per unit time for a same proportion of computing power than *BitcoinCash.* Specifically, when $p_A = 0.35$, the rental fee for *Syscoin* is 163.69 BTC per day whereas that for *BitcoinCash* is 25.84 BTC per day. Nevertheless, *BitcoinCash* requires higher OPEX for profitable DS attacks than *Syscoin*, since the higher λ_H^{-1} of *BitcoinCash* implies the higher γ (the average cost per block mining). In addition, a high λ_H^{-1} proportionally delays the expected AS time.

V. CONCLUSIONS

We showed that DS attacks using 50% or a less proportion of computing power can be profitable. For both the super-50% and the sub-50% proportion regimes, we provided quantitative resources required for profitable DS attacks. Specifically, we provided the probability for an AS success as well as the operating time and expense of mining rigs. We summarized the results in Table I, which enable the easy calculation of the minimum resources required for a profitable attack against any blockchain network. We showed examples of the calculations against working networks.

Our results quantitatively show the importance of network policy. The less the average block mining period and block confirmation number, the less the minimum resources required for a profitable attack. That is to say, blockchain networks pursuing fast transaction speeds are risky. A way for developers of such networks to discourage DS attacks is, for example, to restrict the value of transactions depending on the network policy. If the value of the target transaction is limited below the minimum quantity we provided, attackers cannot expect to make a profit.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] H. Ritzdorf, C. Soriente, G. O. Karame, S. Marinovic, D. Gruber, and S. Capkun, "Toward Shared Ownership in the Cloud," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 12, pp. 3019–3034, Dec. 2018.

[3] S. Wu, Y. Chen, Q. Wang, M. Li, C. Wang, and X. Luo, "CReam: A Smart Contract Enabled Collusion-Resistant e-Auction," *IEEE Trans. Inf. Forensics Secur.*, 2018.

[4] I. Tsabary and I. Eyal, "The Gap Game," in *Proceedings of the 2018 ACM SIGSAC conference on Computer and Communications Security*, 2018, pp. 713–728.

[5] J. A. Kroll, I. C. Davey, and E. W. Felten, "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries," presented at the The Twelfth Workshop on Economics of Information Security (WEIS 2013), Washington, DC, 2013.
[6] B. Biais, C. Bisiere, M. Bouvard, and C. Casamatta, "The Blockchain Folk Theorem," *TSE Work. Pap.*, Jan. 2018.
[7] G.-T. Nguyen and K. Kim, "A Survey about Consensus Algorithms Used in Blockchain," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 101–128, 2018.
[8] Y. Sompolinsky and A. Zohar, "Secure High-Rate Transaction Processing in Bitcoin," presented at the Financial Cryptography and Data Security, Puerto Rico, 2015, pp. 507–527.
[9] A. Beikverdi and J. Song, "Trend of centralization in Bitcoin's distributed network," presented at the 2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Takamatsu, Japan, 2015.
[10] E. Homakov, "Stop. Calling. Bitcoin. Decentralized.," *Egor Homakov*, 03-Dec-2017. [Online]. Available: https://medium.com/@homakov/stop-calling-bitcoin-decentralized-cb703d69dc27.
[11] C. Osborne, "Bitcoin Gold suffers double spend attacks, $17.5 million lost," *ZDNet*, 25-May-2018. [Online]. Available: https://www.zdnet.com/article/bitcoin-gold-hit-with-double-spend-attacks-18-million-lost.
[12] "ZenCash Statement on Double Spend Attack," *Horizen*, 03-Jun-2018. [Online]. Available: https://blog.zencash.com/zencash-statement-on-double-spend-attack/.
[13] A. Hertig, "Blockchain's Once-Feared 51% Attack Is Now Becoming Regular," *CoinDesk*, 08-Jun-2018. [Online]. Available: https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular/.
[14] J. Bonneau, "Why buy when you can rent? Bribery attacks on Bitcoin consensus," presented at the The 3rd Workshop on Bitcoin and Blockchain Research (BITCOIN '16), Barbados, 2016.
[15] M. Rosenfeld, "Analysis of Hashrate-Based Double Spending," *ArXiv14022009 Cs*, Feb. 2014.
[16] G. Bissias, B. N. Levine, A. P. Ozisik, and G. Andresen, "An Analysis of Attacks on Blockchain Consensus," *ArXiv161007985 Cs*, Oct. 2016.
[17] E. Budish, "The Economic Limits of Bitcoin and the Blockchain," Jun-2018. [Online]. Available: http://www.nber.org/papers/w24717.
[18] P.-O. Goffard, "Fraud risk assessment within blockchain transactions," 2018. [Online]. Available: http://pierre-olivier.goffard.me/Publications/FraudRiskAssessmentWithinBlockChainTransaction_Goffard0218.pdf.
[19] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, "Misbehavior in Bitcoin: A Study of Double-Spending and Accountability," *ACM Trans Inf Syst Secur*, vol. 18, no. 1, pp. 2:1–2:32, May 2015.
[20] A. Papoulis and S. U. Pillai, "Random walks and other applications," in *Probability, Random Variables and Stochastic Processes*, 4th edition., Boston, Mass.: McGraw-Hill Europe, 2002.
[21] P. Flajolet and R. Sedgewick, "Combinatorial structures and ordinary generating functions," in *Analytic Combinatorics*, Cambridge University Press, 2009.
[22] G. Gasper and M. Rahman, "Basic Hypergeometric series," in *Basic hypergeometric series*, Second., vol. 96, Cambridge University Press, Cambridge, 2004.
[23] W. Feller, "Random walk and ruin problems," in *An introduction to probability theory and its applications*, New York: Wiley, 1968.
[24] H. S. Wilf, "Analytic and asymptotic methods," in *generatingfunctionology: Third Edition*, 3 edition., Wellesley, Mass: A K Peters/CRC Press, 2005.
[25] H. S. Wilf, "Introductory ideas and examples," in *generatingfunctionology: Third Edition*, 3 edition., Wellesley, Mass: A K Peters/CRC Press, 2005.
[26] P. Flajolet and R. Sedgewick, "Labelled structures and exponential generating functions," in *Analytic Combinatorics*, Cambridge University Press, 2009.

APPENDIX A
PROOF OF COROLLARY 3 AND PROPOSITION 5

A. *Proof of Corollary 3*

We reduce the infinite summations in (15) into an algebraic form using generating functions.

By substituting (16) into (15), the probability $\mathbb{P}_{AS-ICT}$ becomes

$$\mathbb{P}_{AS-ICT}=\sum_{j=N_{BC}}^{2N_{BC}}\binom{j-1}{N_{BC}-1}p_A\sum_{i=2N_{BC}+1}^{\infty}C_{\frac{i-1}{2}-N_{BC},2N_{BC}-j}\left(p_Ap_H\right)^{\frac{i-1}{2}}+\left(\frac{p_H}{p_A}\right)^{N_{BC}}\sum_{i=2N_{BC}+1}^{\infty}\binom{i-1}{N_{BC}-1}{p_A}^{i}. \tag{46}$$

By rearranging the indices i in the summations, we can obtain

$$\mathbb{P}_{AS-ICT}=\sum_{j=N_{BC}}^{2N_{BC}}\binom{j-1}{N_{BC}-1}p_A\sum_{i=0}^{\infty}C_{i,2N_{BC}-j}\left(p_Ap_H\right)^{i+N_{BC}}+\left(\frac{p_H}{p_A}\right)^{N_{BC}}\left(\sum_{i=N_{BC}}^{\infty}\binom{i-1}{N_{BC}-1}{p_A}^{i}-\sum_{i=N_{BC}}^{2N_{BC}}\binom{i-1}{N_{BC}-1}{p_A}^{i}\right). \tag{47}$$

We define two generating functions as

$$M_k(x):=\sum_{i=0}^{\infty}C_{i,k}x^i, \tag{48}$$

and

$$G_k(x):=\sum_{i=k}^{\infty}\binom{i}{k}x^i. \tag{49}$$

By substituting M_k and G_k into (47), we can write

$$\mathbb{P}_{AS-ICT}=\sum_{j=N_{BC}}^{2N_{BC}}\binom{j-1}{N_{BC}-1}p_A\left(p_Ap_H\right)^{N_{BC}}M_{2N_{BC}-j}\left(p_Ap_H\right)+\left(\frac{p_H}{p_A}\right)^{N_{BC}}\left(p_AG_{N_{BC}-1}(p_A)-\sum_{i=N_{BC}}^{2N_{BC}}\binom{i-1}{N_{BC}-1}{p_A}^{i}\right). \tag{50}$$

The function $M_k(x)$ is a generating function of the ballot numbers $C_{i,k}$, for which the algebraic expression given in [24] is

$$M_k(x)=\left(\frac{2}{1+\sqrt{1-4x}}\right)^{k+1}. \tag{51}$$

Putting $x=p_Ap_H$ into $M_k(x)$ results in

$$\begin{aligned}M_k(p_Ap_H)&=\left(\frac{2}{1+\sqrt{1-4p_Ap_H}}\right)^{k+1}\\&=\begin{cases}\left(\frac{2}{1+\sqrt{1-4(1-p_A)p_A}}\right)^{k+1}, & p_A<p_H,\\ \left(\frac{2}{1+\sqrt{1-4(1-p_H)p_H}}\right)^{k+1}, & p_A\geq p_H\end{cases}\\&=\left(\frac{1}{p_M}\right)^{k+1},\end{aligned} \tag{52}$$

where $p_M:=\max(p_H,p_A)$.

$G_k(x)$ is a generating function of binomial coefficients, and the algebraic expression for it is given in [25]:

$$G_k(x)=\frac{x^k}{(1-x)^{k+1}}. \tag{53}$$

Putting $x=p_A$ into $G_k(x)$ results in

$$G_k(p_A)=p_H^{-1}\left(\frac{p_A}{p_H}\right)^k. \tag{54}$$

Substituting (52) and (54) into (50) arrives at

$$\mathbb{P}_{AS-ICT}=\sum_{j=N_{BC}}^{2N_{BC}}\binom{j-1}{N_{BC}-1}p_A\left(p_Ap_H\right)^{N_{BC}}p_M{}^{-(2N_{BC}-j+1)}+1-\left(\frac{p_H}{p_A}\right)^{N_{BC}}\sum_{i=N_{BC}}^{2N_{BC}}\binom{i-1}{N_{BC}-1}p_A{}^{i}. \tag{55}$$

We define $p_m:=\min\left(p_A,p_H\right)$, then the relationship $p_Ap_H=p_mp_M$ holds. By rearranging the order of operands, we can obtain

$$\mathbb{P}_{AS-ICT}=1-\sum_{j=N_{BC}}^{2N_{BC}}\binom{j-1}{N_{BC}-1}\left(\left(\frac{p_H}{p_A}\right)^{N_{BC}}p_A{}^{j}-\frac{p_A}{p_M}\left(\frac{p_m}{p_M}\right)^{N_{BC}}p_M{}^{j}\right), \tag{56}$$

which is equal to (21). ■

B. Proof of Proposition 5

We use the generating functions and their derivatives to compute the infinite summations in (32).

By substituting (16) into (32) and rearranging the order of operands, we obtain

$$\begin{aligned}\lambda_T\mathbb{E}_{T_{AS-ICT}}=&\sum_{j=N_{BC}}^{2N_{BC}}\binom{j-1}{N_{BC}-1}\sum_{i=2N_{BC}}^{\infty}(i+1)C_{\frac{i}{2}-N_{BC},2N_{BC}-j}p_A{}^{\frac{i+2}{2}}p_H{}^{\frac{i}{2}}\\&+\sum_{i=N_{BC}-1}^{\infty}(i+1)\binom{i}{N_{BC}-1}p_A{}^{i+1-N_{BC}}p_H{}^{N_{BC}}\\&-\sum_{i=N_{BC}-1}^{2N_{BC}-1}(i+1)\binom{i}{N_{BC}-1}p_A{}^{i+1-N_{BC}}p_H{}^{N_{BC}}.\end{aligned} \tag{57}$$

By rearranging the indices of summations, we arrive at

$$\begin{aligned}\lambda_T\mathbb{E}_{T_{AS-ICT}}=&\sum_{j=N_{BC}}^{2N_{BC}}\binom{j-1}{N_{BC}-1}p_A{}^{N_{BC}+1}p_H{}^{N_{BC}}\\&\cdot\sum_{i=0}^{\infty}(2i+2N_{BC}+1)C_{i,2N_{BC}-j}\left(p_Ap_H\right)^{i}\\&+p_A\left(\frac{p_H}{p_A}\right)^{N_{BC}}\sum_{i=N_{BC}-1}^{\infty}(i+1)\binom{i}{N_{BC}-1}p_A{}^{i}\\&-\sum_{i=N_{BC}}^{2N_{BC}}i\binom{i-1}{N_{BC}-1}p_A{}^{i-N_{BC}}p_H{}^{N_{BC}}.\end{aligned} \tag{58}$$

By substituting generating functions $M_k(x)$ and $G_k(x)$ defined respectively in (48) and (49), (58) becomes

$$\begin{aligned}\lambda_T\mathbb{E}_{T_{AS-ICT}}=&\sum_{j=N_{BC}}^{2N_{BC}}\binom{j-1}{N_{BC}-1}p_A{}^{N_{BC}+1}p_H{}^{N_{BC}}\\&\cdot\left(2\sum_{i=0}^{\infty}iC_{i,2N_{BC}-j}\left(p_Ap_H\right)^{i}\right.\\&\left.+(2N_{BC}+1)M_{2N_{BC}-j}\left(p_Ap_H\right)\right)\\&+p_A\left(\frac{p_H}{p_A}\right)^{N_{BC}}\left(\sum_{i=N_{BC}-1}^{\infty}i\binom{i}{N_{BC}-1}p_A{}^{i}+G_{N_{BC}-1}\left(p_A\right)\right)\\&-\sum_{i=N_{BC}}^{2N_{BC}}i\binom{i-1}{N_{BC}-1}p_A{}^{i-N_{BC}}p_H{}^{N_{BC}}.\end{aligned} \tag{59}$$

We use the following relationships,

$$\sum_{i=0}^{\infty}iC_{i,k}x^i=xM_k'(x) \tag{60}$$

and

$$\sum_{i=k}^{\infty}i\binom{i}{k}x^i=xG_k'(x), \tag{61}$$

and their derivatives are given by

$$\begin{aligned}M_k'(x):=&\frac{d}{dx}M_k(x)\\=&\sum_{i=0}^{\infty}iC_{i,k}x^{i-1}\\=&\frac{(k+1)}{\sqrt{1-4x}}\left(\frac{2}{1+\sqrt{1-4x}}\right)^{k+2}\end{aligned} \tag{62}$$

and

$$\begin{aligned}G_k'(x):=&\frac{d}{dx}G_k(x)\\=&\sum_{i=k}^{\infty}i\binom{i}{k}x^{i-1}\\=&\frac{\left(kx^{k-1}+x^k\right)}{(1-x)^{k+2}}.\end{aligned} \tag{63}$$

By substituting (60) and (61) into (59), we obtain

$$\begin{aligned}\lambda_T\mathbb{E}_{T_{AS-ICT}}=&\sum_{j=N_{BC}}^{2N_{BC}}\binom{j-1}{N_{BC}-1}p_A{}^{N_{BC}+1}p_H{}^{N_{BC}}\\&\cdot\left(2p_Ap_HM_{2N_{BC}-j}'\left(p_Ap_H\right)+(2N_{BC}+1)M_{2N_{BC}-j}\left(p_Ap_H\right)\right)\\&+p_A\left(\frac{p_H}{p_A}\right)^{N_{BC}}\left(p_AG_{N_{BC}-1}'\left(p_A\right)+G_{N_{BC}-1}\left(p_A\right)\right)\\&-\sum_{i=N_{BC}}^{2N_{BC}}i\binom{i-1}{N_{BC}-1}p_A{}^{i-N_{BC}}p_H{}^{N_{BC}}\end{aligned} \tag{64}$$

Putting $x=p_Ap_H$ into $M_k'(x)$ results in

$$\begin{aligned}M_k'\left(p_Ap_H\right)=&M_k'\left(p_mp_M\right)\\=&\frac{(k+1)}{1-2p_m}\left(\frac{1}{p_M}\right)^{k+2}.\end{aligned} \tag{65}$$

Putting $x=p_A$ into $G_k'(x)$ gives

$$G_k'\left(p_A\right)=\frac{\left(kp_A{}^{k-1}+p_A{}^{k}\right)}{p_H{}^{k+2}}. \tag{66}$$

By substituting (52), (54), (65), and (66) into (64), we finally obtain (33). ■

APPENDIX B
PROOF OF PROPOSITION 4

We use a generating function and generalized hypergeometric functions to compute the infinite summations in (24).

By substituting $\Pr\left(\mathbf{\Delta}_I\in\mathcal{W}_i\right)$ in (16) and $f_{T_i}(t)$ in (25) into (24), we arrive at

$$\begin{aligned}f_{T^{(1),(2)}}(t)-\left(1-\mathbb{P}_{AS-ICT}\right)\delta(t-\infty)=&\sum_{j=2N_{BC}}^{j=2N_{BC}}\binom{j-1}{N_{BC}-1}\sum_{i=2N_{BC}+1}^{\infty}C_{\frac{i-1}{2}-N_{BC},2N_{BC}-j}p_A{}^{\frac{i+1}{2}}p_H{}^{\frac{i-1}{2}}\frac{\lambda_T{}^{i}t^{i-1}e^{-\lambda_Tt}}{(i-1)!}\\&+\sum_{i=2N_{BC}+1}^{\infty}\binom{i-1}{N_{BC}-1}p_H{}^{N_{BC}}p_A{}^{i-N_{BC}}\frac{\lambda_T{}^{i}t^{i-1}e^{-\lambda_Tt}}{(i-1)!}.\end{aligned} \tag{67}$$

By rearranging the indices of summations and the order of operands, we obtain

$$
\begin{aligned}
&f_{T^{(1),(2)}}(t)-(1-\mathbb{P}_{AS-ICT})\delta(t-\infty)= \\
&\sum_{j=N_{BC}}^{j=2N_{BC}}\binom{j-1}{N_{BC}-1}\sum_{i=0}^{\infty}\Big(D_{i,2N_{BC}-j}\,{p_A}^{N_{BC}+i+1}\,{p_H}^{N_{BC}+i} \\
&\qquad\cdot\frac{{\lambda_T}^{2N_{BC}+2i+1}t^{2N_{BC}+2i}e^{-\lambda_T t}}{(2N_{BC}+2i)!}\Big) \\
&+\left(\frac{p_H}{p_A}\right)^{N_{BC}}e^{-\lambda_T t}\left(\sum_{i=N_{BC}}^{\infty}\binom{i-1}{N_{BC}-1}{p_A}^{i}\frac{{\lambda_T}^{i}t^{i-1}}{(i-1)!}\right. \\
&\qquad\left.-\sum_{i=N_{BC}}^{2N_{BC}}\binom{i-1}{N_{BC}-1}{p_A}^{i}\frac{{\lambda_T}^{i}t^{i-1}}{(i-1)!}\right).
\end{aligned}
\tag{68}
$$

We can define two generating functions as

$$
\begin{aligned}
B(x)&:=\sum_{i=0}^{\infty}C_{i,2N_{BC}-j}\frac{x^i}{(2N_{BC}+2i)!} \\
&=(2N_{BC}-j+1)\sum_{i=0}^{\infty}\frac{(2i+2N_{BC}-j)!}{i!(i+2N_{BC}-j+1)!}\frac{x^i}{(2N_{BC}+2i)!},
\end{aligned}
\tag{69}
$$

and

$$
\begin{aligned}
H(x)&:=\sum_{i=N_{BC}}^{\infty}\binom{i-1}{N_{BC}-1}\frac{x^{i-1}}{(i-1)!} \\
&=\sum_{i=N_{BC}-1}^{\infty}\binom{i}{N_{BC}-1}\frac{x^i}{i!}.
\end{aligned}
\tag{70}
$$

By substituting $B(x)$ and $H(x)$ into (68), we obtain

$$
\begin{aligned}
&f_{T^{(1),(2)}}(t)-(1-\mathbb{P}_{AS-ICT})\delta(t-\infty)= \\
&\sum_{j=N_{BC}}^{j=2N_{BC}}\binom{j-1}{N_{BC}-1}p_A\lambda_T e^{-\lambda_T t}\left(p_A p_H(\lambda_T t)^2\right)^{N_{BC}}B\left(p_A p_H(\lambda_T t)^2\right) \\
&+\left(\frac{p_H}{p_A}\right)^{N_{BC}}e^{-\lambda_T t}\left(p_A\lambda_T H(p_A\lambda_T t)-\sum_{i=N_{BC}}^{2N_{BC}}\binom{i-1}{N_{BC}-1}{p_A}^{i}\frac{{\lambda_T}^{i}t^{i-1}}{(i-1)!}\right).
\end{aligned}
\tag{71}
$$

We replace function $B(x)$ in (69) with the generalized hypergeometric functions defined in Appendix E. For this purpose, we first denote the sequences in $B(x)$ by

$$
\beta_i=\frac{(2i+2N_{BC}-j)!}{i!(i+2N_{BC}-j+1)!}\frac{1}{(2N_{BC}+2i)!},
\tag{72}
$$

and

$$
\beta_0=\frac{1}{(2N_{BC}-j+1)(2N_{BC})!}.
\tag{73}
$$

Next, the function $B(x)$ can be rewritten as

$$
\begin{aligned}
B(x)&=(2N_{BC}-j+1)\sum_{i=0}^{\infty}\beta_i x^i \\
&=(2N_{BC}-j+1)\beta_0\left(x^0+\frac{\beta_1}{\beta_0}x^1+\frac{\beta_2}{\beta_1}\frac{\beta_1}{\beta_0}x^2+\cdots\right).
\end{aligned}
\tag{74}
$$

The reformulated sequence in (74) is computed by

$$
\frac{\beta_{i+1}}{\beta_i}=\frac{(i+1+N_{BC}-j/2)(i+1/2+N_{BC}-j/2)}{(i+2+2N_{BC}-j)(i+1+N_{BC})(i+1/2+N_{BC})(i+1)},
\tag{75}
$$

which has 2 polynomials in i on the numerator and 3 polynomials in i on the denominator, except for $(i+1)$. By the definition of the generalized hypergeometric function [22], function $B(x)$ can be expressed as

$$
\begin{aligned}
B(x)&=(2N_{BC}-j+1)\beta_0\ {}_2F_3(\mathbf{a}_j;\mathbf{b}_j;x) \\
&=\frac{1}{(2N_{BC})!}\ {}_2F_3(\mathbf{a}_j;\mathbf{b}_j;x),
\end{aligned}
\tag{76}
$$

where vectors $\mathbf{a}_j$ and $\mathbf{b}_j$ respectively defined in (27) and (28) are the constants in the polynomials in i of the numerator and denominator in (75), respectively.

We use a closed-form expression of generating function $H(x)$ in (70) given by

$$
\begin{aligned}
H(x)&=\sum_{i=N_{BC}-1}^{\infty}\binom{i}{N_{BC}-1}\frac{x^i}{i!} \\
&=\frac{1}{(N_{BC}-1)!}\sum_{i=N_{BC}-1}^{\infty}\frac{x^i}{(i-N_{BC}+1)!} \\
&=\frac{x^{N_{BC}-1}}{(N_{BC}-1)!}\sum_{i=0}^{\infty}\frac{x^i}{i!} \\
&=\frac{x^{N_{BC}-1}}{(N_{BC}-1)!}e^x,
\end{aligned}
\tag{77}
$$

where the following relationship is used [26]:

$$
\sum_{i=0}^{\infty}\frac{x^i}{i!}=e^x.
\tag{78}
$$

By substituting (76) and (77) into (67), we arrive at

$$
\begin{aligned}
&f_{T^{(1),(2)}}(t)-(1-\mathbb{P}_{AS-ICT})\delta(t-\infty)=\frac{p_A\lambda_T e^{-\lambda_T t}\left(p_A p_H(\lambda_T t)^2\right)^{N_{BC}}}{(2N_{BC})!} \\
&\quad\cdot\sum_{j=N_{BC}}^{j=2N_{BC}}\binom{j-1}{N_{BC}-1}\ {}_2F_3\left(\mathbf{a}_j;\mathbf{b}_j;p_A p_H(\lambda_T t)^2\right) \\
&\quad+\left(\frac{p_H}{p_A}\right)^{N_{BC}}e^{-\lambda_T t}\left(p_A\lambda_T\frac{(p_A\lambda_T t)^{N_{BC}-1}}{(N_{BC}-1)!}e^{p_A\lambda_T t}\right. \\
&\qquad\left.-\sum_{i=N_{BC}}^{2N_{BC}}\binom{i-1}{N_{BC}-1}{p_A}^{i}\frac{{\lambda_T}^{i}t^{i-1}}{(i-1)!}\right) \\
&=\frac{p_A\lambda_T e^{-\lambda_T t}\left(p_A p_H(\lambda_T t)^2\right)^{N_{BC}}}{(2N_{BC})!} \\
&\quad\cdot\sum_{j=N_{BC}}^{j=2N_{BC}}\binom{j-1}{N_{BC}-1}\ {}_2F_3\left(\mathbf{a}_j;\mathbf{b}_j;p_A p_H(\lambda_T t)^2\right) \\
&\quad+\left(\frac{p_H}{p_A}\right)^{N_{BC}}e^{-\lambda_T t}\left(p_A\lambda_T\frac{(p_A\lambda_T t)^{N_{BC}-1}}{(N_{BC}-1)!}e^{p_A\lambda_T t}\right. \\
&\qquad\left.-\frac{1}{(N_{BC}-1)!}\sum_{i=N_{BC}}^{2N_{BC}}{p_A}^{i}\frac{{\lambda_T}^{i}t^{i-1}}{(i-N_{BC})!}\right).
\end{aligned}
\tag{79}
$$

We obtain (26) by rearranging the indices of the summations and the order of operands. ■

APPENDIX C
PROOF OF THEOREM 7

When $x_1=x_2$, $x_3=x_4$, $r_1=r_2$, and $r_3=r_4$, the OPEX and block mining reward respectively turn into

$$
X(\lambda_A,T_{AS})=\gamma\lambda_A T_{AS}
\tag{80}
$$

and

$$
R(\lambda_A,T_{AS})=\beta\lambda_A T_{AS}.
\tag{81}
$$

Combining these conditions implies that expected OPEX $\mathbb{E}_X$ defined in (39) becomes

$$
\begin{aligned}
&\mathbb{E}_X(p_A,t_{cut};N_{BC}) \\
&=\mathbb{P}_{AS}(p_A,t_{cut};N_{BC})\gamma\lambda_A\mathbb{E}_{T_{AS}}(p_A,t_{cut};N_{BC}) \\
&\quad+(1-\mathbb{P}_{AS}(p_A,t_{cut};N_{BC}))\gamma\lambda_A t_{cut}.
\end{aligned}
\tag{82}
$$

For $p_A \in (0, 0.5)$, $\mathbb{P}_{AS} < 1$ always holds, since $\mathbb{P}_{AS} \le \mathbb{P}_{AS-ICT}$ by the definition and $\mathbb{P}_{AS-ICT} < 1$ by (21). Thus, if $t_{cut} = \infty$, the expected OPEX in (82) diverges to minus infinity. In other words, the expected profit $\mathbb{E}_P$ in (38) with $p_A \in (0, 0.5)$ is positive only if $t_{cut} < \infty$.

We next derive the sufficient and necessary condition (41) for $p_A \in (0.5, 1)$ and $t_{cut} = \infty$. When $t_{cut} = \infty$, $T_{AS} = T_{AS-ICT}$ and $\mathbb{P}_{AS} = \mathbb{P}_{AS-ICT}$ by the definition of AS-ICT. In addition, $p_A \in (0, 0.5)$ implies $\mathbb{P}_{AS-ICT} = 1$ by (21). In this case, by substituting (80) and (81), the expected profit $\mathbb{E}_P$ in (38) becomes

$$\mathbb{E}_P(p_A, \infty; N_{BC}) = C + (\beta - \gamma)\lambda_A \mathbb{E}_{T_{AS-ICT}}(p_A; N_{BC}). \quad (83)$$

Hence, $\mathbb{E}_P > 0$ if and only if the value C of target transaction is greater than $C_{\text{Req.}}$ given in (41). ■

APPENDIX D
PROOF OF THEOREM 8

We obtain an upper bound $C_{\text{Suf.}}$ of $C_{\text{Req.}}$ in (40). If $C > C_{\text{Suf.}}$ then $C > C_{\text{Req.}}$, which implies that a DS attack $\mathcal{A}(C, p_A, c\mathbb{E}_{T_{AS-ICT}}; N_{BC})$ for a positive real number c is profitable.

As $\mathbb{E}[R(\lambda_A, T_{AS})]$ in (40) is nonnegative by the definition of function R, we arrive at the upper bound:

$$C_{\text{Req.}} \le \frac{\mathbb{E}_X(p_A, t_{cut}; N_{BC})}{\mathbb{P}_{AS}(p_A, t_{cut}; N_{BC})}. \quad (84)$$

By substituting $t_{cut} = c\mathbb{E}_{T_{AS-ICT}}$, $x_1 = x_2$, and $x_3 = x_4$, the expected OPEX $\mathbb{E}_X$ in (84) becomes

$$\begin{aligned}\mathbb{E}_X(p_A, c\mathbb{E}_{T_{AS-ICT}}; N_{BC}) = {} & \mathbb{P}_{AS}(p_A, c\mathbb{E}_{T_{AS-ICT}}; N_{BC})\gamma\lambda_A \mathbb{E}_{T_{AS}} \\ & + \left(1 - \mathbb{P}_{AS}(p_A, c\mathbb{E}_{T_{AS-ICT}}; N_{BC})\right)\gamma\lambda_A c\mathbb{E}_{T_{AS-ICT}}.\end{aligned} \quad (85)$$

We use the following relationship on the conditional expectation

$$\begin{aligned}\mathbb{E}_{T_{AS}} &= \frac{\int_0^{t_{cut}} t f_{T^{(1)(2)}}(t)\,dt}{\mathbb{P}_{AS}(p_A, t_{cut}; N_{BC})} \le \frac{\lim_{x \to \infty^-} \int_0^x t f_{T^{(1)(2)}}(t)\,dt}{\mathbb{P}_{AS}(p_A, t_{cut}; N_{BC})} \\ &= \frac{\mathbb{P}_{AS-ICT}(p_A; N_{BC})}{\mathbb{P}_{AS}(p_A, t_{cut}; N_{BC})} \mathbb{E}_{T_{AS-ICT}}(p_A; N_{BC}).\end{aligned} \quad (86)$$

By substituting (85) and (86) into (84), we finally obtain the upper bound $C_{\text{Suf.}}$ given in (42). ■

APPENDIX E
THE GENERALIZED HYPERGEOMETRIC FUNCTION

A generalized hypergeometric series [22] is a power series $\sum_{n \ge 0} \beta_n z^n$, where the ratio of coefficients are expressed by polynomials $A(n)$ and $B(n)$ in n as follows:

$$\frac{\beta_{n+1}}{\beta_n} = \frac{A(n)}{B(n)(n+1)}, \quad (87)$$

for all integers $n \ge 0$. The polynomials are written by

$$A(n) = c(a_1 + n)\cdots(a_p + n) \quad (88)$$

and

$$B(n) = d(b_1 + n)\cdots(b_q + n). \quad (89)$$

The generalized hypergeometric series is denoted by

$${}_pF_q(\mathbf{a}; \mathbf{b}; z), \quad (90)$$

where $\mathbf{a}$ and $\mathbf{b}$ are vectors of $a_1, \cdots, a_p$ and $b_1, \cdots, b_q$, respectively.

A generalized hypergeometric series defines a generalized hypergeometric function if it converges. If $p < q + 1$, then the ratio of coefficients (87) goes to zero as $n \to \infty$, which implies that the series converges for any finite value z and thus defines the function.