Profitable Double-Spending Attacks & Prevention

Jehyuk Jang and Heung-No Lee

Department of electrical engineering and computer science, GIST

GIST

광주과학기술원

Gwangju Institute of Science and Technology

- 1995년 대학원 개원
- 2010년 학부 개설
- 학생 10 : 교수 1
- 학부 총원 718명
- 대학원 총원 1282명
- 박사과정 졸업생 SCI급 저널 5.93편

세계 속의 GIST

세계 3위
교수 1인당 논문 피인용 수
(QS 세계대학평가)

국내 1위
기술이전 수입
(한국경제)

최우수그룹
4년제대학 창업지수 평가
(매경이코노미)

국내 9위 / 세계 315위
종합순위(QS 세계대학평가)

국내 3위 / 세계 32위
설립 50년 미만 대학평가 (QS 세계대학평가)

국내 4위/ 세계 41위
설립 50년 미만 대학평가(THE 세계대학평가)

국내 2위
특허 출원·등록 수(한국경제)
교원1인당 연구비(한국연구재단)

국내 8위
세계에서 가장 혁신적인(톰슨로이터)

GIST
교육환경

학생 전원
납입금·장학금 수혜

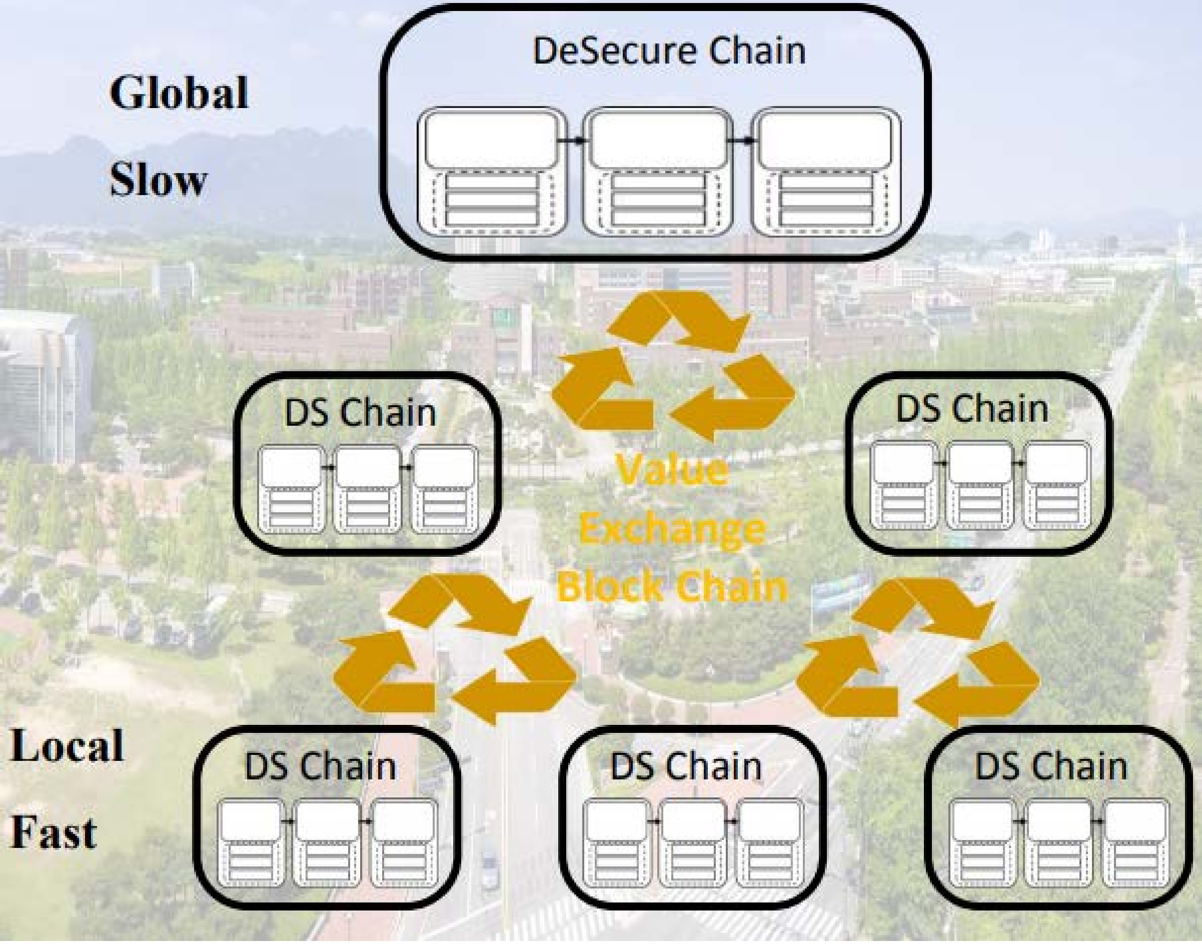
학생 100%
기숙사 지원

전공과목
100% 영어 강의

Gwangju Institute of Science and Technology
Blockchain Economy Center

DeSecure chains are

1) Highly secure
2) Highly Decentralized
3) TPS Adjustable



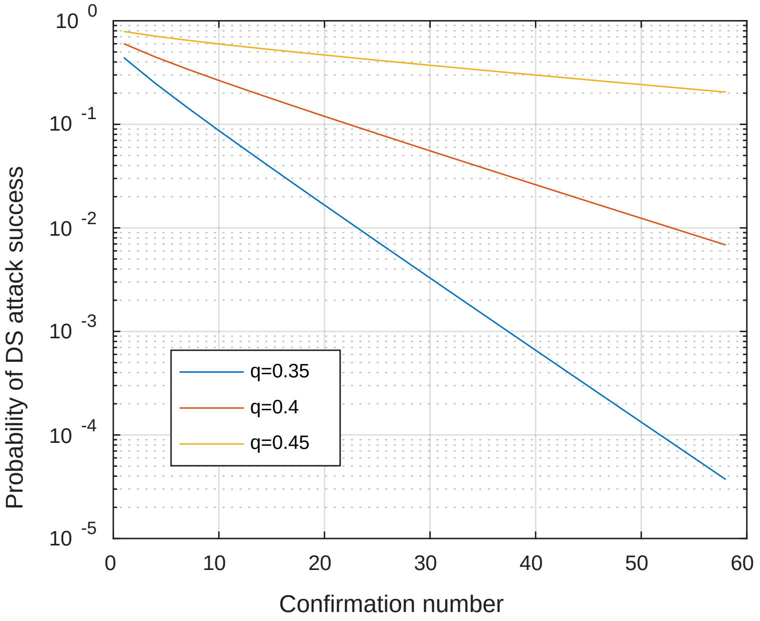
The aim is
to build and distribute
the DeSecure chains
under GIST OSL.

Please contact us via
https://infonet.gist.ac.kr/
heungno@gist.ac.kr

Goal

Q) For safe blockchain transaction,
how many block confirmations are required?

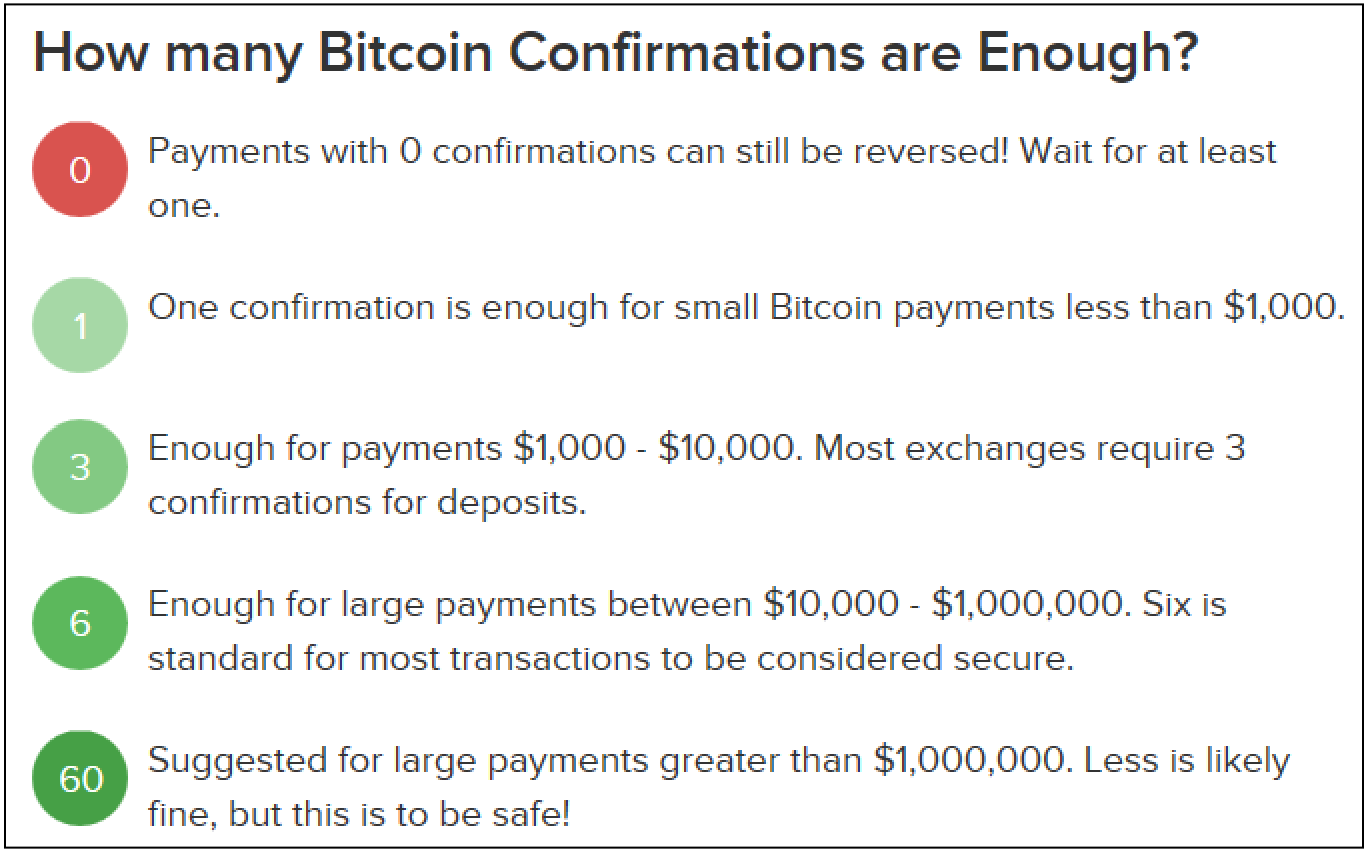
- In Bitcoin white paper, “more confirmations implies less probability of DS attack success,” *Satoshi Nakamoto*.



- However, it’s still unclear that how many confirmations are required to ensure my transaction **SAFE**?

A recent (2019) guideline on Bitcoin confirmations

https://www.buybitcoinworldwide.com/confirmations/



How many Bitcoin Confirmations are Enough?

0 Payments with 0 confirmations can still be reversed! Wait for at least one.

1 One confirmation is enough for small Bitcoin payments less than $1,000.

3 Enough for payments $1,000 - $10,000. Most exchanges require 3 confirmations for deposits.

6 Enough for large payments between $10,000 - $1,000,000. Six is standard for most transactions to be considered secure.

60 Suggested for large payments greater than $1,000,000. Less is likely fine, but this is to be safe!

Are you sure? Do you agree with this?

Other similar guidelines

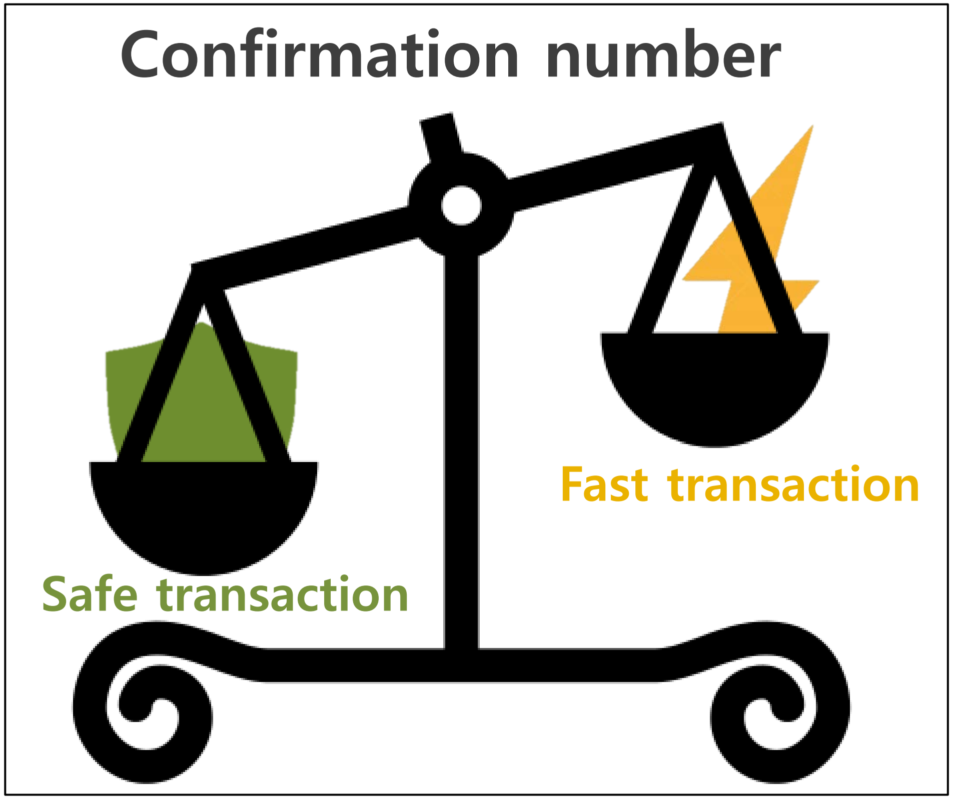
- https://www.ethos.io/what-are-blockchain-confirmations/
- https://coincentral.com/blockchain-confirmations/
- https://blog.monetha.io/confirmation/
- https://support.coinjar.com/hc/en-us/articles/115005712843-Reasons-for-a-pending-Bitcoin-transfer

- Blockchain communities agree with the importance confirmations.
- Yet, they all have suggested abstract confirm. numbers.
- No one has suggested reasonable confirm. numbers.

Why do we need a clearer guideline on confirmations?

A good confirmation number:

1. ensures safe transaction, and
2. keeps fast transaction

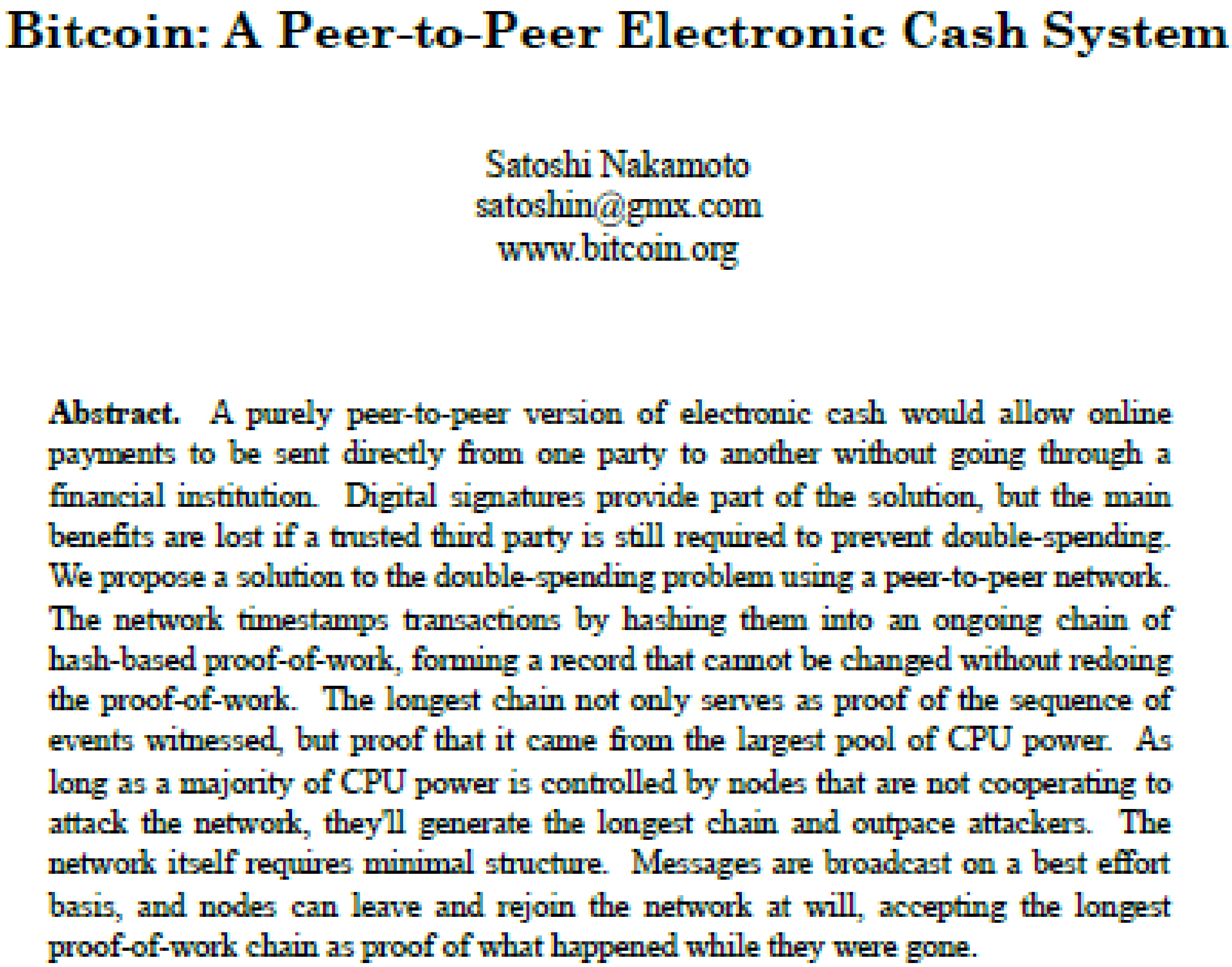


Presentation Outline

- **Review of**
  - Blockchain (Bitcoin)
  - Double-Spending (DS) Attack

- **New Analysis Results: Profitable DS Attacks**

- **Algorithm to Prevent Profitable DS Attacks**

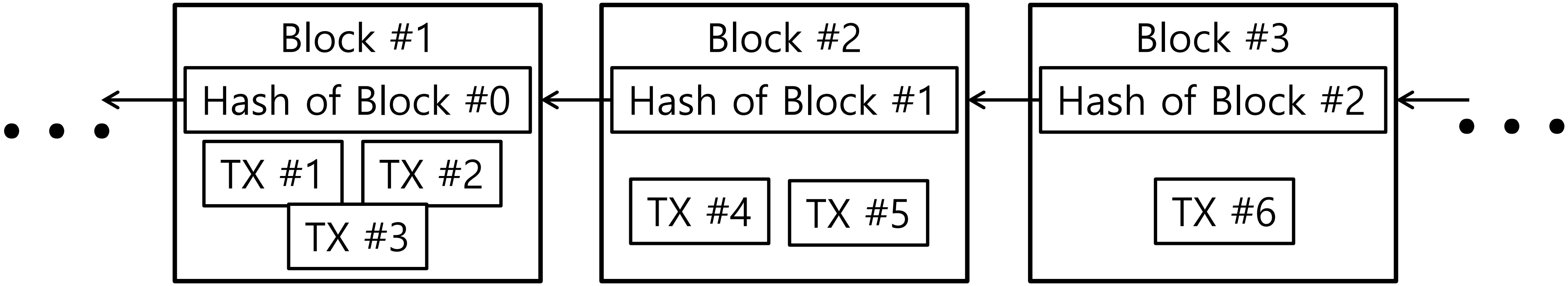


Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Blockchain

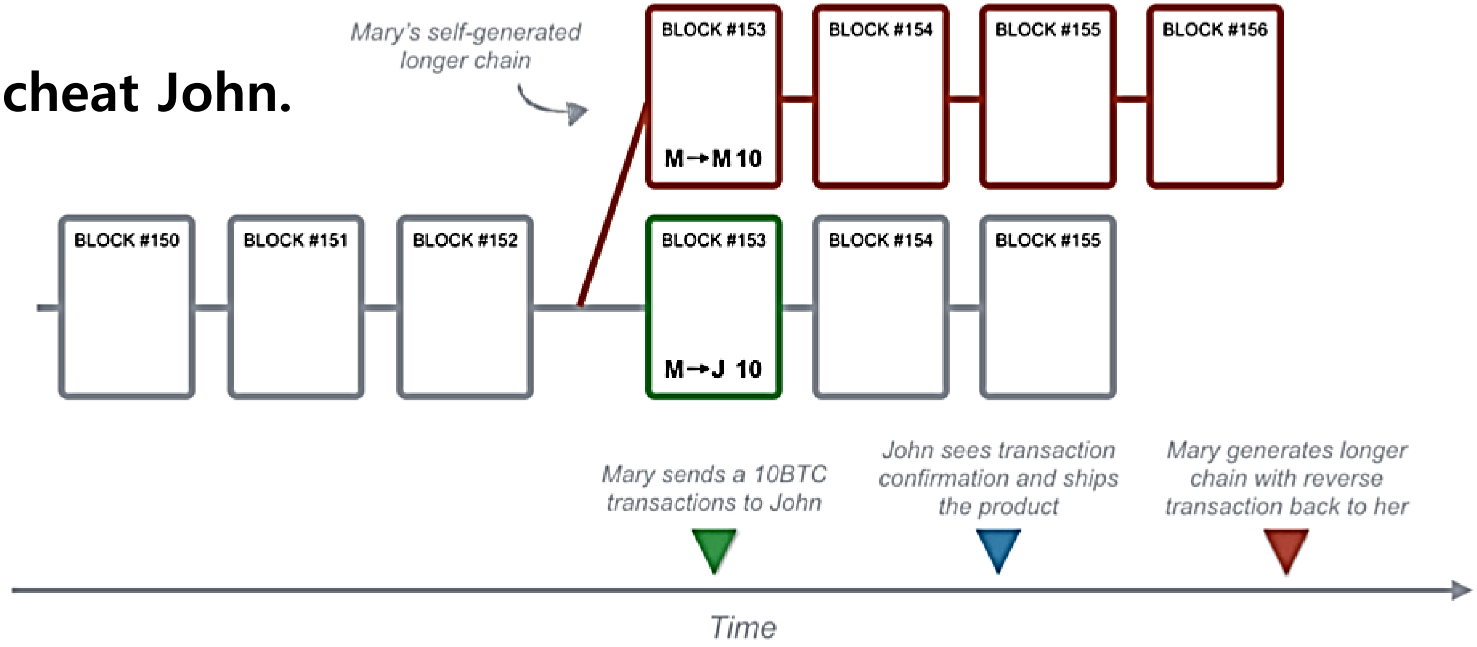


***Blockchain** is a **chain** of blocks.*

- Data immutability?
  - **By the chain of PoW**
- Double-spending?
  - **By directed graph of TX in/out**
- Consensus?
  - **Longest-chain rule (Bitcoin)**
  - **A variant of GHOST (Ethereum)**

Double-Spending Attack

Mary can cheat John.
But how?


Mary's self-generated longer chain
BLOCK #153
M→M 10
BLOCK #154
BLOCK #155
BLOCK #156
BLOCK #150
BLOCK #151
BLOCK #152
BLOCK #153
M→J 10
BLOCK #154
BLOCK #155
Mary sends a 10BTC transactions to John
John sees transaction confirmation and ships the product
Mary generates longer chain with reverse transaction back to her
Time

1. Target transaction: "Mary sends 10 BTC to John," put in **Block #153**.
2. Miners build the public chain (gray).
3. Mary builds her own chain underground (red).
4. Mary's chain contains a **fake transaction** that nullifies the target transaction.
5. Mary divulges her fake chain to the public if
   1) John has completed shipping the product to Mary, AND
   2) Mary's fake chain has been built longer than the public's chain.
6. The public adopts Mary's chain, since it is longer than their own chain.

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., 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 expected attack cost and expected attack success time. 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% and 40% proportions of computing power against *Syscoin* and *BitcoinCash* networks, and quantitatively shown how vulnerable they are.**

***Index Terms*— Blockchain, Bitcoin, Double-Spending**

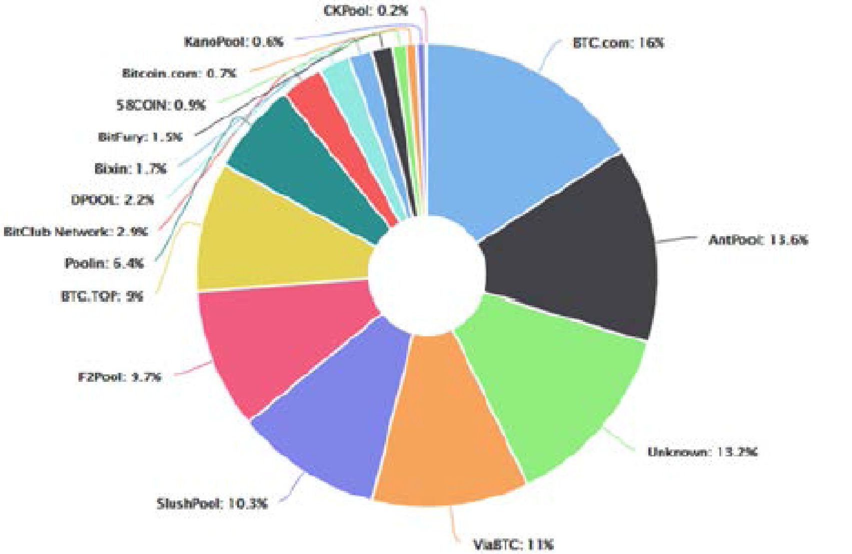


Fig. 1. Computation power distribution among the largest mining pools provided by *blockchain.com* (date accessed: 22 Oct. 2018).

succeeds in generating a new block, he/she has the latest version of the chain. All of the peers continuously communicate with each other to share the latest chain. If a peer 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

Paper Goal

- To analyze the profitability of double-spending (DS)

- Satoshi Nakamoto,

  “DS attack is **difficult** since its success **requires 51%** of total computing power.”

- We show

  DS attacks are **threatening even** with **less than 50%**.

Definitions

Notation	Description
p_A	Attacker’s portion of computing power (0~100%)
N_{BC}	Block confirmation number of target transaction
t_{cut}	Attack cut time for cut loss

***Definition*.** A DS attack succeeds if

- target transaction has got confirmed by N_{BC} blocks,
- Mary’s chain has grown longer than the public chain, and
- **the above two conditions have been satisfied within a cut time** t_{cut}.

Nakamoto's result

- The probability that double-spending attack will *ever* succeed:

$$\mathbb{P}_{AS} = 1 - \sum_{k=0}^{N_{BC}} \frac{\lambda^k e^{-\lambda_H}}{k!} \left(1 - \begin{cases} 1 & if \;\; p_A \geq 0.5 \\ \left(p_A / (1 - p_A) \right)^{N_{BC} - k} & if \;\; p_A < 0.5 \end{cases} \right).$$

If Mary has p_A **greater** than 50% and **no cut time** $t_{cut} = \infty$, then double-spending attack succeeds.

- According to this result, double-spending attack seems very difficult.

- However, Nakamoto's result does not say

$$\boxed{p_A < 50\% \;\; \overset{?}{\Rightarrow} \;\; \begin{array}{l}\text{Profitable DS Attack} \\ \text{is impossible.}\end{array}}$$

Our results (Main)

***Definition*.** A DS attack is *profitable* if and only if the expected revenue is greater than the expected cost.

※ Revenue: cheating value of target transaction
※ Cost: operating expense for computing hash functions

***Theorem*.** For all attacker's fractions of computing power p_A (1%~99%), DS attacks are profitable if the value V of target transaction is greater than

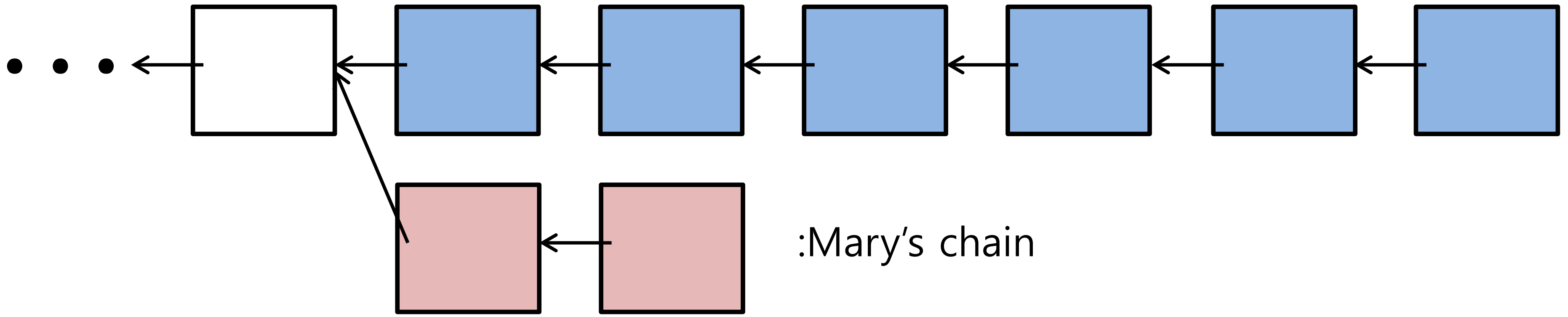
$$V_{Suf.}(p_A; N_{BC}) = \gamma'(p_A) \frac{\lambda_H p_A \mathrm{E}[T_{AS}]}{(1-p_A)\mathbb{P}_{AS}(p_A, t_{cut}; N_{BC})}.$$

Even though p_A **is less than** 50% ,
Mary can expect a profitable DS attack.

Our results (2)

Theorem. A DS attack using p_A less than 50% are profitable only if a finite cut time $t_{cut} < \infty$ is given.

- Example)

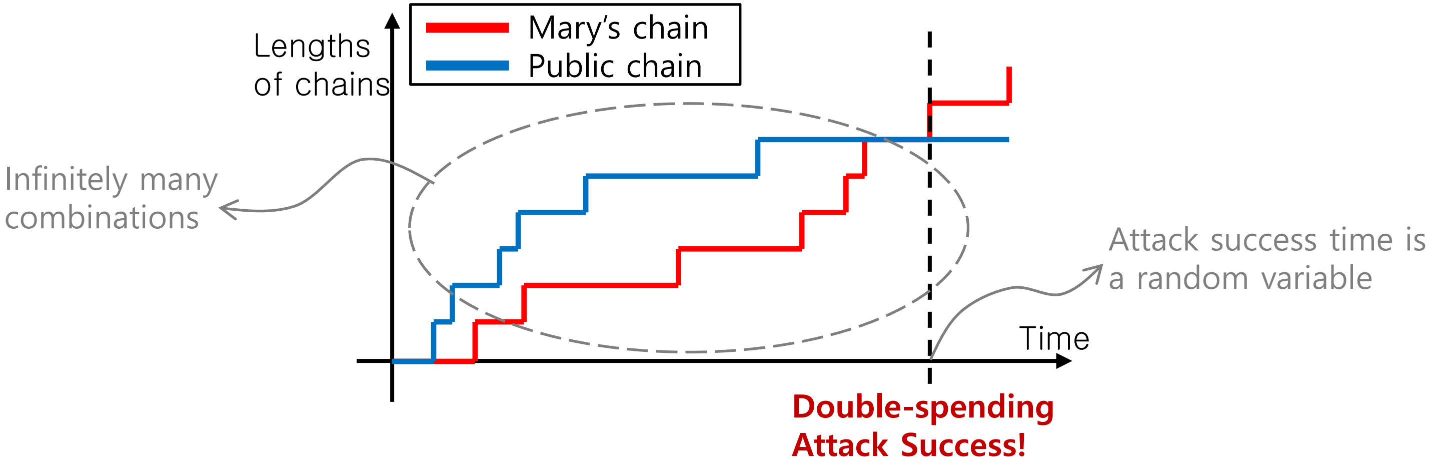


- ➢ The probability that Mary's chain NEVER catch up the public chain is nonzero.
- ➢ If there is no time limit and Mary's chain never catch up the public chain, the operating expense increases infinitely.
- ➢ Thus, Mary should stop the attack at a cut time to cut loss.

Our results (3)

We provide the probability density function of attack success time.

- ➢ DS attack is modeled as a competition of two Poisson processes.
- ➢ There are infinitely many combinations of the two Poisson processes which implies the success of a DS attack.
- ➢ We count the probabilities of such infinite combinations using combinatorics and generating functions.

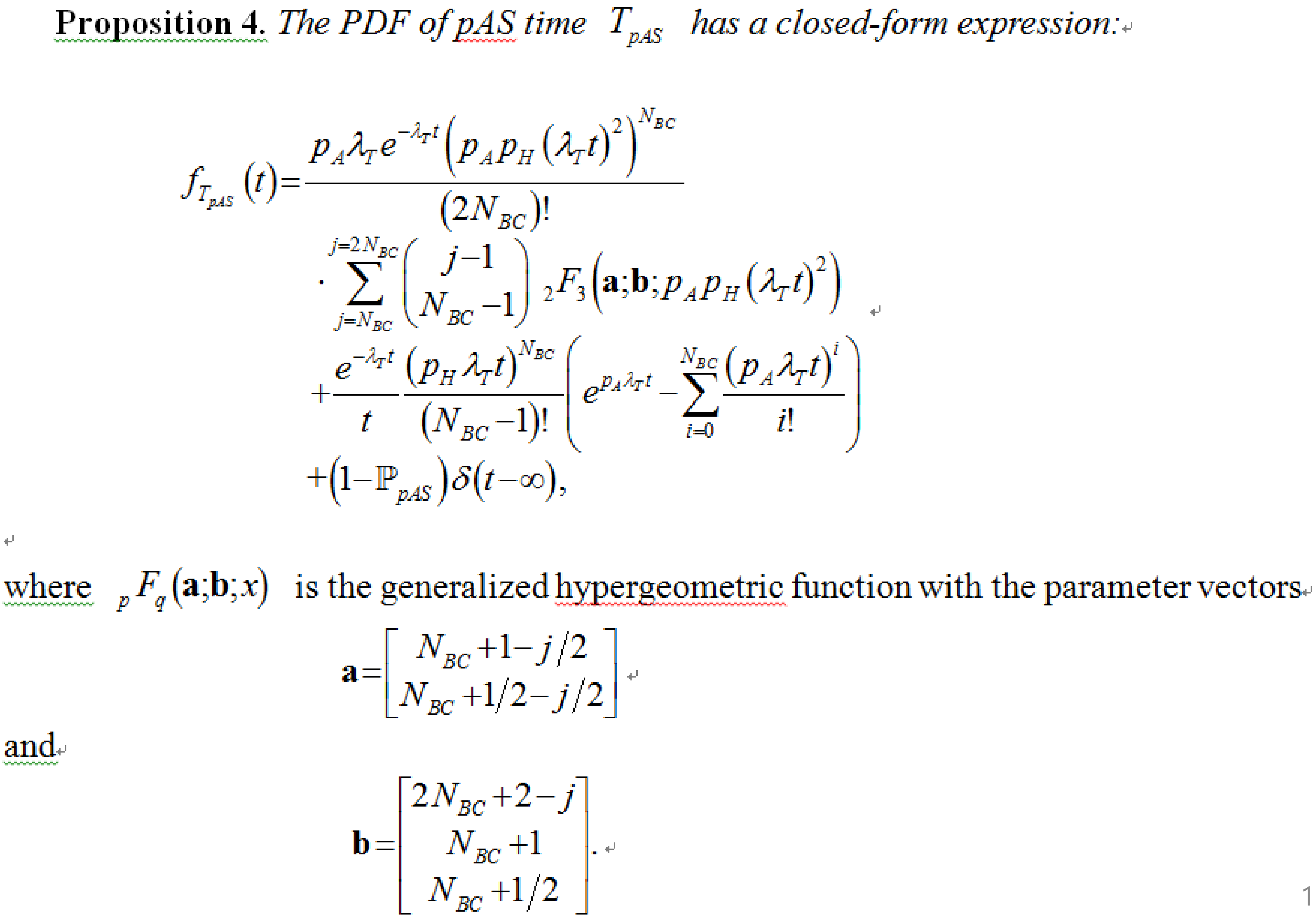


Infinitely many combinations

Attack success time is a random variable

Double-spending Attack Success!

Our results (3)



Proposition 4. *The PDF of pAS time* T_{pAS} *has a closed-form expression:*

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

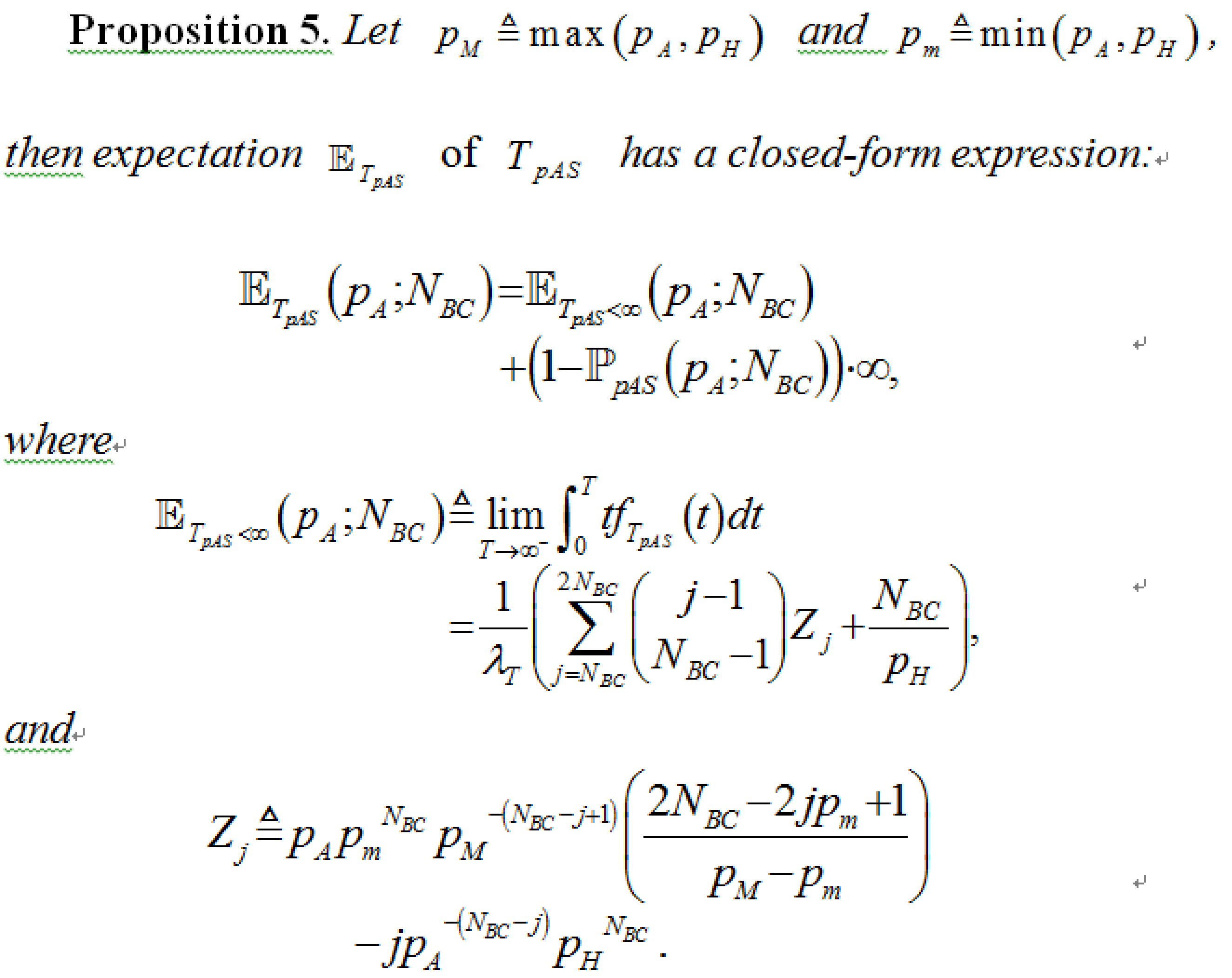
where ${}_pF_q(\mathbf{a};\mathbf{b};x)$ is the generalized hypergeometric function with the parameter vectors

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

and

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

Our results (3)



Proposition 5. *Let* $p_M \triangleq \max(p_A, p_H)$ *and* $p_m \triangleq \min(p_A, p_H)$,

then expectation $\mathbb{E}_{T_{pAS}}$ of T_{pAS} *has a closed-form expression:*

$$\mathbb{E}_{T_{pAS}}(p_A;N_{BC}) = \mathbb{E}_{T_{pAS}<\infty}(p_A;N_{BC}) + \left(1-\mathbb{P}_{pAS}(p_A;N_{BC})\right)\cdot\infty,$$

where

$$\mathbb{E}_{T_{pAS}<\infty}(p_A;N_{BC}) \triangleq \lim_{T\to\infty^-}\int_0^T t f_{T_{pAS}}(t)\,dt = \frac{1}{\lambda_T}\left(\sum_{j=N_{BC}}^{2N_{BC}}\binom{j-1}{N_{BC}-1}Z_j + \frac{N_{BC}}{p_H}\right),$$

and

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

Example of Profitable DS Attack in *BitcoinCash* network

BitcoinCash Info.

- The amount of TXs over 24 hours is about 10 billion dollars.
- Miners' average block generation time (λ_H^{-1}) is fixed to 600secs.

Mary's Info.

- Average block generation time: 1143secs (p_A =35%)
- Attack cut time (t_{cut}): 3hours 36mins
- Operating cost per time: γ

Attack Info.

- Value of target transaction: V
- Block confirmation number (N) of target transaction: 5
- Attack success probability within the cut time: 22%
- Expected attack success time(T_{AS})(if attack succeeded): 1hour 42mins

Profit Info.

- Expected revenue: $0.22 * V$
- Expected cost: 0.22*(1hour 42mins)*γ+0.78*(3hours 36mins)*γ
- Profit=(expected revenue)-(expected cost)

Example of Profitable DS Attack in *BitcoinCash* network

Profit Info.

- ➢ Expected revenue: $0.22 * V$
- ➢ Expected cost: 0.22*(1hour 42mins)*γ+0.78*(3hours 36mins)*γ
- ➢ Profit=(expected revenue)-(expected cost)

- How to make attack profitable?

Make target value V so that Profit>0.

- ➢ The operating expense per time (γ) is given in internet.
- ➢ For example, *nicehash.com* provides a rental service of computing power.
- ➢ According to nicehash.com, the **expected cost is 2.909 BTC.**

If $V > 13.225$ BTC, this attack is profitable.

(when attack power is 0.35 and confirmation number is 5)

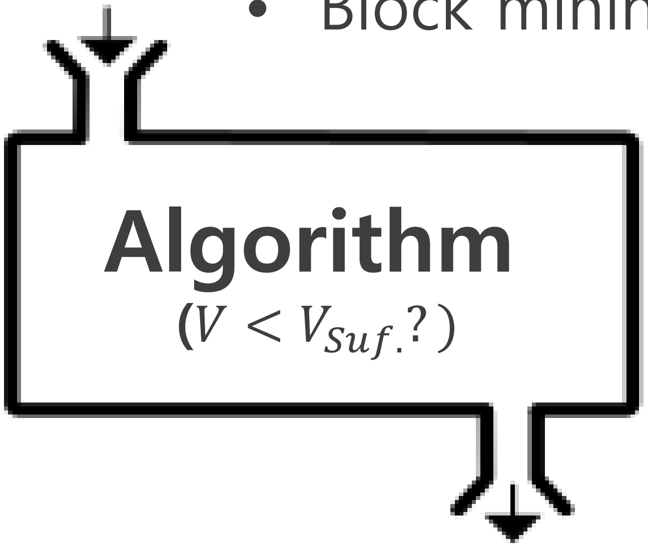
Mathematical Tool to Check Risk of Double-Spending Attack

Your TX info.:

- TX value (V),
- Confirmation number

Network info.:

- Average block mining period
- Block mining cost
- Block mining reward



Algorithm

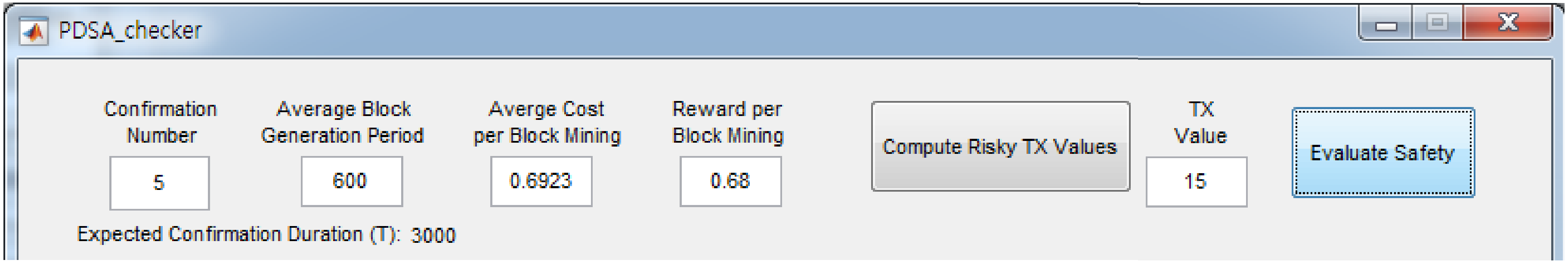
($V < V_{Suf.}?$)

"Your TX is **SAFE** (or) **NOT SAFE."**

Example) The BitcoinCash Network Parameters (ref: BTC.com, nicehash.com as of Apr. 2019)

- **Average block mining period: 600 Seconds**
- Total hash: 2.48 [EHashes/second]
- **Block mining reward: 0.68 [BTC/block mining]**
- Block mining hash: 1488 [EHashes/block mining]
- SHA256 cost: 0.0402 [BTC/(PHashes/sec)/day]
  = 4.6527*10^-7 [BTC/PHashes]
  = 4.6527*10^-22 [BTC/Hash]
- **Block mining cost:** 4.6527*10^-22 [BTC/Hash]
  *1488*10^18 [Hashes/Block mining]
  = **0.6923 [BTC/block mining]**

Evaluate the safety!



Confirmation Number: 5

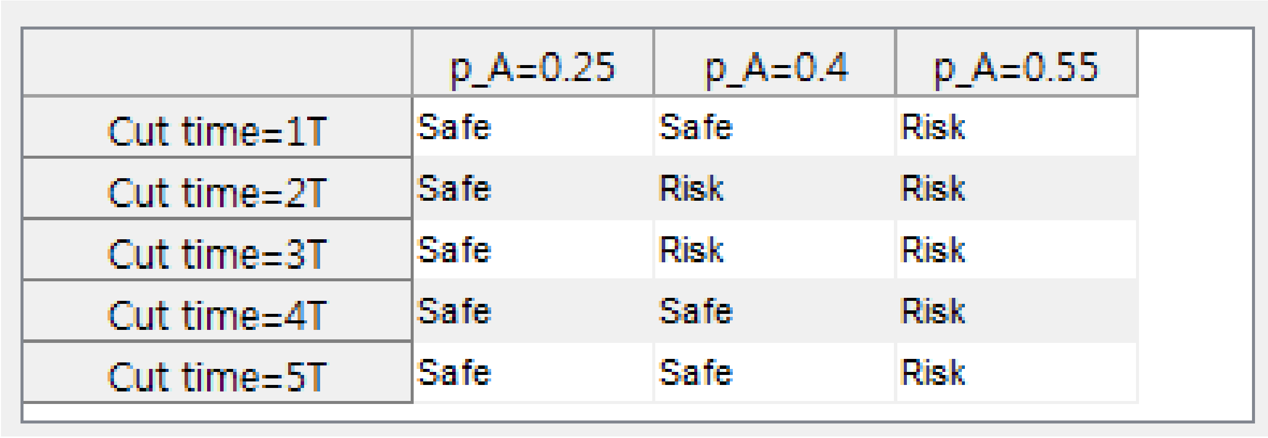
Average Block Generation Period: 600

Averge Cost per Block Mining: 0.6923

Reward per Block Mining: 0.68

TX Value: 15

Expected Confirmation Duration (T): 3000



	p_A=0.25	p_A=0.4	p_A=0.55
Cut time=1T	Safe	Safe	Risk
Cut time=2T	Safe	Risk	Risk
Cut time=3T	Safe	Risk	Risk
Cut time=4T	Safe	Safe	Risk
Cut time=5T	Safe	Safe	Risk

Comparison of guidelines

	Nakamoto's	Ours
Input	Attacker's computing power	• Attacker's computing power • **Transaction information** • **Network information**
Output	Attack success probability	**Binary decisions** (safe or not)
Math. Tools	Attack success probability	• Attack success probability • Attack cost • Attack success time
Remark	Against attacks with computing power more than 51%, every transaction is always vulnerable.	Even for attacks with computing power more than 51%, it is possible to make transactions safe.

Summary

We provide new analyses on DS attacks such as

1. probabilistic behaviors of attack success time and
2. conditions for profitable DS attacks.

They enabled our new results such as

1. riskiness of DS attacks even with less than 50% of computing power and
2. a clearer guideline on confirmations.

Thank you

contact: jjh2014@gist.ac.kr
heungno@gist.ac.kr