2018 5th International Conference on Information, Cybernetics,
and Computational Social Systems (ICCSS)

A Sustainable Reward Mechanism for Block Mining in PoW-based Blockchain

Feilong Lin, Zhonglong Zheng, Zhiliang Huang, Changbing Tang, Hao Peng, and Zhongyu Chen
College of Mathematics, Physics and Information Engineering, Zhejiang Normal University, Zhejiang, P. R. China
Email: {bruce_lin, zhonglong, zlhuang, tangcb, hpeng, czy}@zjnu.cn

***Abstract*—Blockchain brings a peer-to-peer transaction solution without a trusted third authority over the peer-to-peer network. Proof-of-work (PoW), also called 'mining', incents some peers (called miners) to compete for the right of block generation by rewarding a certain mount of cryptocurrency. Hence, PoW undertakes the cryptocurrency creation and block generation in a blockchain based transaction system (BTS). However, in a BTS, the block mining reward (BMR) will be terminated after that the regulated quantity of currency have been minted. Although the voluntarily paid transaction fee is allowed to support BMR, the stable reward for block mining is no longer guaranteed, and which inevitably destroys the sustainability of BTS.**

In this work, we propose a sustainable reward mechanism (SRM) for block mining in BTS. Specifically, SRM introduces a mandatory transaction fee mechanism with dedicated fee rate determination algorithm. An on-chain public account (PA), which is trust-free but security-provable, is set to collect the dynamic transaction fees. With transaction fee collection under adaptive fee rate setting, PA provides the steady BMR, thus makes blockchain sustainable when the currency creation purposed BMR has been terminated. Numerical results are presented to demonstrate the effectiveness of SRM.

***Index Terms*—Blockchain, block mining, sustainable reward**

I. Introduction

The development of network technologies encountering the blooming peer-to-peer businesses gave the birth of blockchain, which brought a peer-to-peer transaction solution without the necessitation of a trusted third authority or central server [1, 2]. Blockchain has attracted much attention from various domains, e.g., sharing financial [3], transparent stock market [4], healthcare intelligence [5], industry security [6], secure internet of things [7, 8], personal data security [9] etc.. Technically, blockchain constructs a distributed ledger consisting of time labeled and ordered data blocks. Over blockchain running network, normally a peer-to-peer network, each block with all of the contained transactions must be validated across the network according to predefined rules. Only the successfully validated block can be added to the ledger and locally restored by the nodes. This process is also referred as distributed consensus. Distributed consensus together with time ordered records guarantees the validity and irreversibility of the distributed ledger, i.e., blockchain. Besides, cryptological technologies, such as public key encryption and digital signature, are integrated into the blockchain protocol, which enable the security of private information and cryptocurrency payment during the peer-to-peer transaction. Another cryptography based technology, named proof-of-work (PoW), is used to control the block generation. Specifically, some network nodes, called miners, use their computing power to solve the difficulty-controllable hash puzzle. The miner, who firstly acquires the answer, gains the right to generate a new block by packing all of the collected transactions into it. After that the fresh block has been validated cross the network and added to the blockchain, miners start to mine next block and also start the new round of blockchain generation.

Block mining reward (BMR), incents the miners working for block mining, thus to keep the steady generation of blocks and makes the blockchain based transaction system (BTS) sustainable. For example, Bitcoin [1], a well known BTS, formulates a cash reward mechanism. When a block is generated, the corresponding miner will get a certain cryptocurrency from Bitcoin system, i.e., bitcoins (BTC), as the mining reward. It is noted that this systematic reward, the currency creation purposed reward, is exactly the unique origin of the cryptocurrency. That is why the generation process of the block is vividly called as block mining. Specifically, the BMR in Bitcoin system starts at 50 BTC and halves every $210,000$ blocks. Finally, the total BTC will be hold at the level of 21 million [10]. That is because to guarantee the stability of economic ecosystem, the amount of currency in a BTS are necessary to be limited. In another word, the currency creation purposed reward for block mining in preliminary phase of BTS has to be terminated after that the regulated quantity of currency have been issued.

It can be foreseen that a direct consequence of BMR reduction or termination is the collapse of BTS, since that the stable block mining process cannot be maintained. To avoid this consequence, an extensively accepted transaction cost mechanism [10] is introduced into the blockchain. When the miner gains the right to generate a block, he can get reward from transaction fees provided by the payers of transactions. However, there are still several shortages of the existing transaction cost mechanism. First, transaction fees are voluntarily paid by users, thus the earning of miners is hard to be stably guaranteed. Even if no transaction fee is paid during one block generation period, the miner gains nothing. Second, transaction occurrence is not periodic or even dramatically fluctuating, and the consequent reward formed by transaction fees cannot protect periodic generation of chain blocks. In this context, the smooth reward of block mining is no longer guaranteed which inevitably destroys the stability of economic ecosystem. Therefore, how to stabilize the BMR after BTS reaching

978-1-5386-7088-0/18/$31.00 ©2018 IEEE

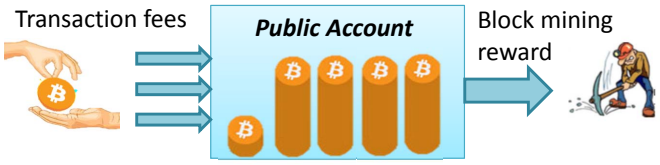

Fig. 1. Public account for transaction fees collection and block mining reward payment in SRM.

TABLE I
STRUCTURE OF THE GENERATION TRANSACTION INVOLVING PA

Field	Description
Transaction Hash	All bits are zero
Output Index	All bits are ones
Coinbase Data Size	From 2 to 100 bytes
Coinbase Data	Arbitrary data
• {Balance}	The balance of the PA up to this block
• {Fee rate}	The transaction fee rate in next block generation period
Sequence Number	Set to 0xFFFFFFFF

the regulated currency issuance is an open and significantly important issue.

This paper proposes a sustainable rewarding mechanism (SRM) for BTS. SRM suggests that users in BTS pay a mandatory fee for each transaction according to predefined fee rate. In particular, a public account (PA) is set to collect the transaction fees instead of depositing them to miners account directly. The miner who successfully mines the new block will draw a fixed reward from the PA, e.g., 25 BTC in Bitcoin system. The reliability and security of the PA can be guaranteed by the validity and irreversibility of blockchain. The design of SRM and its security statements are presented in Section II. From economic sense, transaction fee rate is significantly important for economic ecosystem [11]. Rational transaction fee rate setting makes PA neither plunder superfluous currency nor become tight to pay for the BMR. The mathematical model for SRM running and the optimal determination of transaction fee rate are presented in Section III. The performance validations are presented in Section IV.

We summarize the contributions of this work as follows:

1) A sustainable rewarding mechanism (SRM) is proposed. SRM introduces a revenue supported BMR, which can be used to compensate the mining reward when systematic reward is low or replace the currency creation purposed reward when it is terminated.
2) In particular, a trust-free but security-provable public account is introduced to collect transaction fees and pay for BMR. PA is supposed to collect the random and dynamic transaction fees and output a constant BMR.
3) A transaction fee rate determination algorithm is designed, which integrates the slip-window average method for transaction volume estimation and double-threshold control for PA balance stability and sustainability.

For reading convenience, the abbreviations used in this paper are listed as follows in alphabetical order: BMR short for block mining reward, BTC short for bitcoin, BTS short for blockchain based transaction system, PoW short for proof-of-work, PA short for public account, SRM short for sustainable rewarding mechanism.

II. SRM: A SUSTAINABLE REWARDING MECHANISM FOR BLOCKCHAIN

The purpose of SRM is to make the BTS sustainable when the currency creation purposed reward is reduced or terminated. The philosophy of SRM is to introduce a revenue by setting a transaction cost mechanism to replace the currency creation purposed BMR. SRM sets a PA to buffer and balance collected transaction fees and BMR payment, as illustrated in Fig. 1. Accordingly, the core of SRM is to set a trust-free but security-provable PA charging for BMR payment, and then make an appropriate transaction fee rate to balance the revenue and expenditure of the PA. This section presents the SRM design and its security statement. The latter issue, determination of the transaction fee rate, will be discussed in the following section.

A. Design of SRM

The design of SRM is divided into two parts, i.e., the PA and the associated SRM protocol, which are presented as follows.

1) Design of PA: To support the SRM, the targeted PA is required to : 1) collect transaction fees and pay for BMR at the generation of each block in an transparent way and; 2) work in a decentralized manner since that any central entity is not expected in blockchain. Note that personal account or digital wallet has been programmed in BTS, where the digital keys (behalf of the ownership of the cryptocurrency) are stored. However, this personal account is not suitable to be the PA since it is usually off-line and requires a personal signature when paying the money.

In this work, we set the PA as a data structure, which is integrated into coinbase data of the generation transaction of a block. Note that coinbase data has a variable data size and can be used by the miner to write arbitrary data [10]. The structure of the generation transaction containing the PA is shown in Table I. In this structure, the field balance is used to record the remaining money of the PA up to this block, where the transaction fees and BMR payment for this block have also been settled. Another field, fee rate, regulates the proportion that has to be paid as the cost of each transaction in the next block generation period. The determination of the fee rate will be discussed in Section III.

The introduced PA is such a data structure in the block ledger, which is an on-chain account. Hence, no central entity to underlay the PA is needed. The management of PA, i.e., the statistics of balance and the calculation of fee rate in next block generation period, is charged by the incumbent miner of this block according to some rules, which are included in SRM protocol presented as follows.

2) Design of SRM protocol: SRM protocol is developed to regulate the transaction fee payment, validation, and collection, as well as the BMR payment and validation. We state

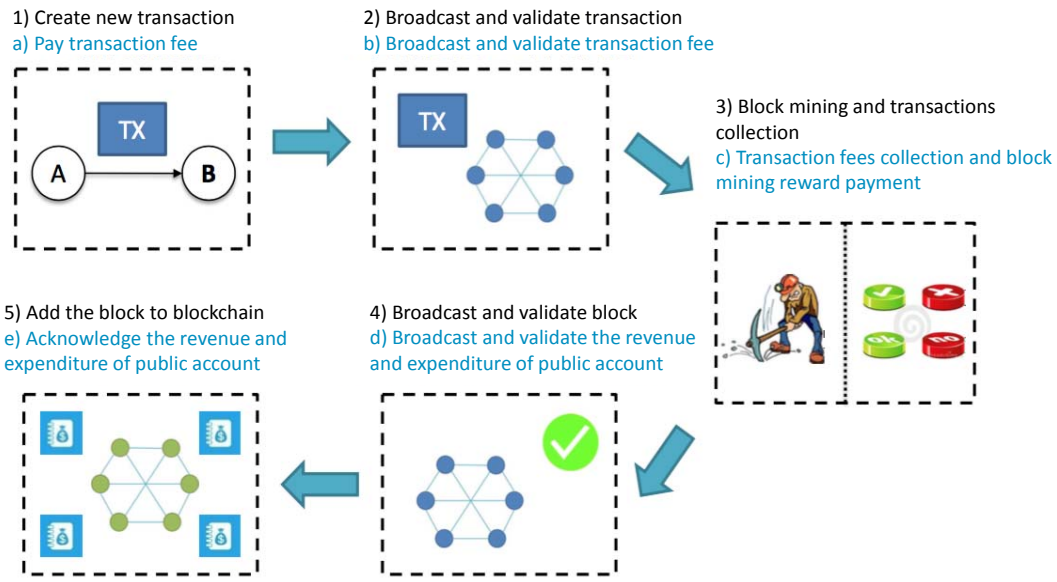

Fig. 2. Illustration of the workflow of SRM, where items 1)∼5) show the flow of block generation and items a)∼e) correspondingly show the flow of the sustainable rewarding mechanism.

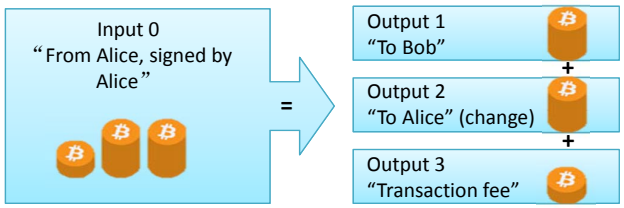

Fig. 3. Schematic diagram of transaction form with SRM

the SRM protocol step by step in a synchronization with the process of block generation. Fig. 2 shows the schematic diagram of SRM, where items 1)∼5) show the flow of block generation and items a)∼e) correspondingly show the flow of SRM. As shown in Fig. 2, SRM protocol consists of five steps, as follows.

Step a) Transaction fee payment: When a user in BTS creates a transaction, he must pay the transaction fee according to the stated fee rate in latest block. Fig. 3 shows the transaction form. Transaction output is divided into three parts. Output 1 is the trading payment transferred to the counterparty. Output 2 is the change transferred back to the user[1]. Output 3 is the transaction fee to be collected into PA. Taking transaction in Fig. 3 as an example, Transaction fee can be calculated by *Output3=Output1*Fee_rate*. The money distribution should satisfy *Input0-Output1*(1+Fee_rate)=Output2*. After the payment setting, the user sends to transaction information to BTS.

Step b) Transaction fee validation across network: Any node (including miners, the same hereinafter) in the blockchain network receives the transaction information, it will validate the transaction according to blockchain protocols. For SRM protocol, the node will verify whether the amount of the outputs equals to the input amount and whether the transaction fee is set according to the regulated fee rate[2]. Only both of the two conditions are satisfied, the node will broadcast this transaction information to its neighbors; otherwise, the transaction will be discarded.

Step c) Transaction fees collection and BMR payment: The miner collects and validates the transactions broadcasted over the blockchain network. If the miner successfully obtains the solution of the mathematical puzzle set by system, it will pack all of the validated transactions into a block. In addition, the miner charges to sum the transaction fees to the balance of PA. The miner also draws the BMR[3] from the PA and deposits it into its own account. The miner finally updates the balance of PA. The fee rate for the next period of block generation is also updated by the miner according to a given algorithm. When the block is ready, the miner transmits it to the blockchain network.

Step d) Validation of revenue and expenditure of PA: Any node in the blockchain network receives the new block, it will validate the block according to blockchain protocols. Also, it will validate the revenue and expenditure of the PA including

[1]The change exists in BTS because that the used cryptocurrency references a specific previous transaction as its source. Hence, the change has to be deposited into a new address when the source is divided.

[2]SRM protocol here is some different from the Bitcoin system in the transaction validation. In Bitcoin system, it requires transaction input amount is larger than the output amount (consisting of transaction payments and the change). The part except the output is considered as the fee to the miner.

[3]Although different transaction volumes may be involved in blocks, the value of each block is identical from the perspectives of PoW and the contribution of maintaining the blockchain. Hence, it is rational to set a constant BRM during a long period.

the collected transaction fees, balance of PA, BMR drawn by the miner of this block, and the fee rate stated by the miner. If the block is successfully validated, the node will transmit the block to its neighbors; otherwise, this block will be discarded.

Step e) Acknowledgement of revenue and expenditure of PA: Any node successfully has validated the new block, it can add the new block to the chain of blocks if it tends to store and update the blockchain. When most of network nodes have confirmed the new block, the revenue and expenditure of PA have also been acknowledged.

B. Statement of the security of SRM

Security is the prominent feature of blockchain. The distributed consensus over large-scale network make the blockchain reliable and hard to be falsfied. All of the results recorded by each block are strictly validated according to the predefined checking criteria. For SRM, security is the prerequisite. In this part, we statement the security of SRM, which is established on distributed consensus process of blockchain.

In BTS, unspent transaction outputs (UTXOs) are indivisible chunks of bitcoin currency locked to a specific owner, recorded on the blockchain, and recognized as currency units by the entire network [10]. When transaction occurs, the payer references a previous transaction recording his UTXO and uses his signature to unlock this UTXO. Then, the currency declared by this UTXO is divided into three parts, where first part is transferred to the counterparty, second part is transferred back to the payer as the change, and third part, if voluntarily paid, is claimed by the block miner as transaction fee. Note that the transaction in BTS allows multiple UTXOs referenced by payer and also multiple counterparties as the payees. After reaching the consensus, the new block declares that the previous UTXO has been spent and the new UTXOs have been formed which belong to the roles above.

In SRM, a new data structure named PA is introduced to the coinbase data in the generation transaction of a block. It also bring some differences from traditional transaction protocols. The transaction fee is mandatory in SRM, and which is collected into PA but not directly paid to block miner. In detail, during the transaction, two divisions of the referenced UTXO, i.e., payment to counterparty and change back to payer, are formed to new UTXOs. However, the third division, i.e., mandatorily paid transaction fee, is not necessarily formed to new UTXO immediately. Instead, only the volume of transaction fee is accumulated and recorded to the balance of PA by the block miner. On the other hand, the block miner generates a new UTXO containing a fixed currency volume for itself as the BRM, and balance of PA is subtracted by same volume of BMR. Besides, block miner also charges to update the fee rate using statistical transaction information according to a certain statistical algorithm. All of the transaction fee collection, BRM payment, and fee rate determination have to be validated via the consensus process of blockchain, as the five steps shown in Fig. 2. Upon finishing the consensus, the previous UTXO of payer cannot be drawn back and spent again, the balance of PA is validated to be effective, and the BRM payment is recognized. Therefore, applying SRM to BTS, we claim

Claim 1: SRM is secure, which has identical security level of BTS.

III. Determination of transaction fee rate in SRM

To complete SRM, an appropriate transaction fee rate is to be determined. Consider that transactions occur randomly which results in a dynamic transaction fee collection. To support the steady BMR, the varying transaction fee rate is suggested to be adopted. Details are presented in the following.

Let $x(k)$ denote the balance of PA at kth block generation period. $s(k)$ denotes the total transaction volume, which is dynamic since the transactions in BTS randomly occur. μ is the constant BMR. As we know, the amount of currency in BTS is large, e.g., tens of millions in Bitcoin system. Hence, we reasonably assume $\mathbf{E}[s(k)] \gg \mu$. Let $\lambda(k)$ denote the transaction fee rate. Then, at $(k+1)$th block generation period, the state transition equation satisfies

$$x(k+1) = x(k) + \lambda(k+1)s(k+1) - \mu. \tag{1}$$

For a rational PA, the balance should not increase to infinite, but should keep the balance not empty. The purpose is to find the appropriate transaction fee rate $\lambda(k)$, thus the following two conditions hold

$$\mathbf{E}[\lambda(k)s(k)] = \mu, \tag{2}$$

$$X_L < x(k) < X_H, \tag{3}$$

where condition (3) further expects the balance of PA to be kept in a given range (X_L, X_H).

For condition (2), the key problem is to acquire the estimate of $s(k+1)$ with the historical information up to kth block. In this work, the slip-window average algorithm, a simple but effective one, is utilized. Let the window length be L. The output of slip-window average, i.e, the estimate of $s(k+1)$, can be formulated as

$$\hat{s}(k+1) = \frac{\sum_{i=0}^{L-1} s(k-i)}{L}. \tag{4}$$

Then, the transaction fee rate in next block generation period, $\lambda(k+1)$, can be determined by

$$\lambda(k+1) = \frac{\mu}{\hat{s}(k+1)}. \tag{5}$$

As for the second condition (3), the double-threshold method is applied. If the balance $x(k)$ has become lower than low threshold, the transaction fee rate $\lambda(k+1)$ will be increased, e.g., increased by 5%. On the contrary, if the balance $x(k)$ has become higher than high threshold, the transaction fee rate $\lambda(k+1)$ will be decreased. The slip-window average algorithm integrated with double-threshold control is presented by Algorithm 1. The double thresholds X_L and X_H are used to keep the balance in a predefined range, thus PA has the capability to pay for BMR continuously.

Algorithm 1 Transaction fee rate determination of SRM

Input: $\{s(k-i)\}, i = 0, 2, \cdots, L-1$; $x(k)$;
Output: $\lambda(k+1)$;
Define: low threshold X_L; high threshold X_H; fee rate increment δ;
Calculate estimate of transaction volume $\hat{s}(k+1)$ according to (4);
Calculate transaction fee rate $\lambda(k+1)$ according to (5);
Adjust transaction fee rate using double-threshold control:
if $x(k) < X_L$ **then**
    $\lambda(k+1) \leftarrow \lambda(k+1) * (1+\delta)$;
else if $x(k) > X_H$ **then**
    $\lambda(k+1) \leftarrow \lambda(k+1) * (1-\delta)$;
else
    $\lambda(k+1) \leftarrow \lambda(k+1)$;
end if

IV. Numerical Analysis

In this part, numerical simulations are conducted to evaluate SRM. Suppose that the transactions occurs randomly. The mean transaction volume is 10000 BTC. The double thresholds are set to $X_L = 500$ and $X_H = 1000$. The BMR is set to be constant, i.e., $\mu = 25$. The fee rate increment used in simulations is $\delta = 5\%$. We simulate the SRM by setting different window lengths, $L = [10, 100, 1000]$, respectively. 10,000 block generation periods are conducted, and the results are presented as follows.

Simulation results first show the effectiveness of SRM in stabilization of balance. Fig. 4 compares the balance variation under constant fee rate setting and slip-window average based fee rate settings. The so called constant fee rate assumes that we have the knowledge of mean transaction volume and directly set the fee rate to 0.25%. In detail in the figure, 'CFR' represents the constant fee rate setting. 'SWA:L=xxx' represents the slip-window average based fee rate setting with 'xxx' window length. In later figures, 'SWA-DT:L=xxx' will be used, which means the double-threshold control is applied. The results in Fig. 4 show that with simple constant fee rate setting, the balance of PA is not stable, which is greatly affected by the real-time transaction volume. Slip-window average uses the average in a configurable past duration to estimate the transaction volume and the corresponding transaction fee rate. It is expected to reduce the influence of transaction dynamics. The simulation results show that balance variation can be improved by slip-window average. Especially, when $L = 10$, the balance variation is much smoother than CFR. It demonstrates that slip-window average method can stabilize the balance of PA. However, if a big window length is selected, the fee rate variation is small which approximates to CFR, and the balance dynamic becomes intensive. In addition, the balance shown in Fig. 4 can fall below zero, which are not expected in SRM.

Before solving the problem of balance falling below zero, we discuss the transaction fee rate variation with different

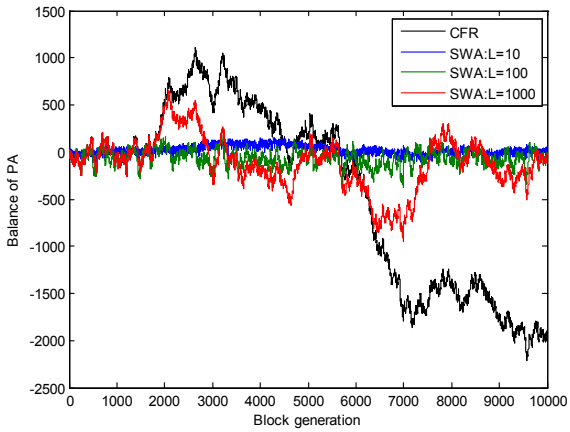

Fig. 4. Balance of PA under constant fee rate and slip-window average based fee rate settings.

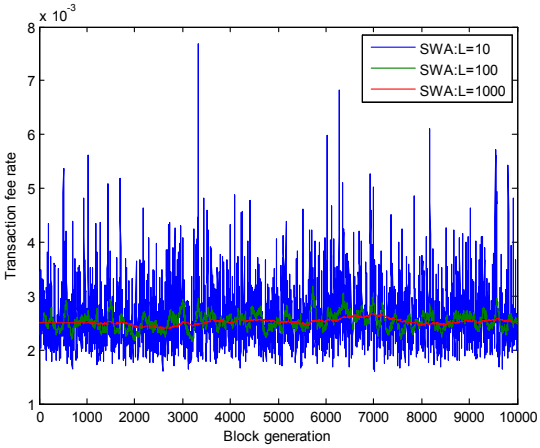

Fig. 5. Slip-window average based fee rates with different window lengths.

window length settings. Fig. 5 shows the results of fee rate variation. As previous description, the fee rate variation is affected by the window length. The mean and standard deviation of fee rate under different window length settings are listed in Table II. The mean fee rate is approximate to constant fee rate 25%. However, the standard deviation is much different with each other. A bigger window length is set, a smaller standard deviation of fee rate is obtained, which means that a much smoother fee rate is resulted. It can well promote the fairness of transaction fee payments in BTS, which is important for the health of BTS. By synthesizing the results in Fig. 5 and Table II, there is a tradeoff between the balance stability and fee rate stability. The setting of $L = 100$ gains a balanced performance than the other two settings of window length.

In the following, the capability to control the range of balance with the double-threshold is demonstrated. The simulation results of balance variation of PA with double-threshold control are shown in Fig. 6. In simulations, the initial balance of PA is set to be zero. With the extra increment of fee rate, i.e., increased by 5% when the balance is lower than X_L,

TABLE II
STATISTICS OF THE MEAN AND STANDARD DEVIATION OF FEE RATE.

	$L = 10$	$L = 100$	$L = 1000$
Mean	0.2605%	0.2522%	0.2512%
Standard deviation	0.0536%	0.0157%	0.0052%

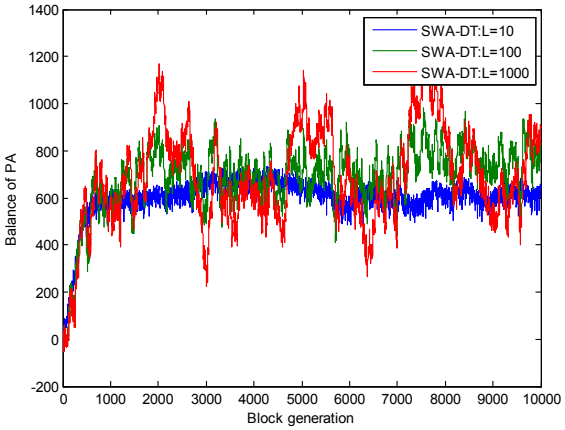

Fig. 6. Balance of PA under the slip-window average based fee rate settings with double-threshold control.

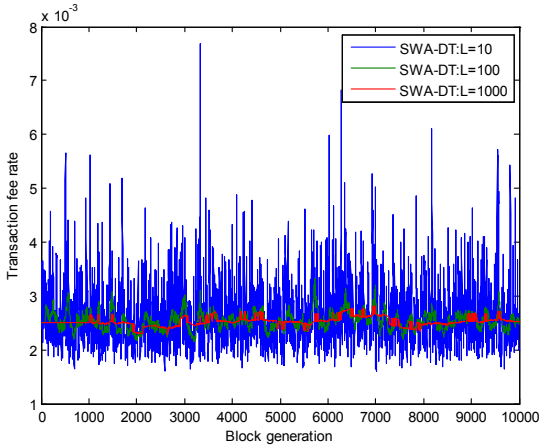

Fig. 7. Slip-window average based fee rates with double-threshold control.

TABLE III
STATISTICS OF THE MEAN AND STANDARD DEVIATION OF FEE RATE UNDER DOUBLE-THRESHOLD CONTROL.

	$L = 10$	$L = 100$	$L = 1000$
Mean	0.2612%	0.2527%	0.2511%
Standard deviation	0.0543%	0.0165%	0.0081%

the balance quickly increases at the beginning of simulations. After that, the balance of PA is almost kept in the predefined range $[X_L,\ X_H]$ when window length is 10 or 100. When $L = 1000$, the fee rate adapts slowly and the balance varies in a big range. However, the balance is still kept above zero. Hence, it can be concluded that double-threshold control effectively stabilizes the balance of PA in SRM.

With double-threshold control, the transaction fee rates under different window length settings are presented in Fig. 7. Similar to Fig. 5, different window lengths are selected, different fee rate dynamics are resulted. Combining the statistics of mean and standard deviation in Table III, a suitable window length brings a balanced performance. For example, when $L = 100$, the balance can be well kept in the predefined range, as well as that the fee rate is relatively stable.

V. CONCLUSION

In this paper, the sustainability of block mining in blockchain has been considered. To deal with the descending or termination of currency creation purposed block mining reward, the sustainable rewarding mechanism is proposed. In this mechanism, transaction fee is mandatorily paid according to a predefined fee rate and collected to the on-chain public account. The balance of the public account is used to pay for block mining reward. The security of the proposed sustainable rewarding mechanism is proved. Simulation results demonstrates that SRM provides a steady block mining reward, thus make the blockchain sustainable.

ACKNOWLEDGEMENT

This work was supported in part by NSF of China under the grant 61672467 and 61503343, and NSF of Zhejiang Province of China under the grants LY18F030013 and LY16F030002.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf, 2008.
[2] M. Swan, *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.
[3] M. Mainelli, M. Smith *et al.*, "Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)," *The Journal of Financial Perspectives*, vol. 3, no. 3, pp. 38–69, 2015.
[4] L. Lee, "New kids on the blockchain: How bitcoin's technology could reinvent the stock market," *Hastings Bus. LJ*, vol. 12, pp. 81–591, 2016.
[5] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, no. 10, p. 218, 2016.
[6] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial internet of things," *Journal of Software Engineering and Applications*, vol. 9, no. 10, p. 533, 2016.
[7] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of things, blockchain and shared economy applications," *Procedia Computer Science*, vol. 98, pp. 461–466, 2016.
[8] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[9] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. 2015 IEEE Security and Privacy Workshops (SPW)*. San Jose, CA, USA: IEEE, May 21-22 2015, pp. 180–184.
[10] A. M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies*. O'Reilly Media, Inc., 2014.
[11] N. G. Mankiw, *Principles of macroeconomics*. Cengage Learning, 2014.