ORIGINAL RESEARCH

E-commerce payment model using blockchain

Shee-Ihn Kim[1] · Seung-Hee Kim[1] 🅾

Abstract
The current e-commerce payment systems for credit or check cards require a payment gateway (PG). This incurs PG fees, which in turn increases the cost of engaging in e-commerce. This paper proposes a simple payment model that uses basic cryptocurrency features, such as public key, private key, and digital signature, to eliminate the need for transaction intermediaries such as public key certificate and PG. This model can process e-commerce payments without registering additional public key certificate, public key, or private key. The use of a digital signature guarantees the integrity and nonrepudiation of electronic payments, besides eliminating the fees for intermediary services such as PG, thereby reducing the overall cost of operating e-commerce services. This proposal is crucial as it is the first attempt to apply blockchain technology to e-commerce payment services. In addition, our model is important because it not only supports the evolution of e-commerce payment technology but also enhances the competitive advantage of using e-commerce.

Keywords Blockchain · e-commerce · Payment gateway · Digital signature

1 Introduction

Prevalence of smartphones and credit cards, evolution of wireless telecommunication networks, and expansion of online shopping are factors propelling the continued growth of the e-commerce market. With this trend, purchasing behaviors are diversifying, along with product sales and delivery, whose methods are evolving into the future. e-commerce is a system comprising suppliers, products, web domains, online shopping malls (websites), servers, payment systems, product delivery systems, and consumers. As the key determinant of consumers' purchase intent is trust (Thompson et al. 2019), the payment system is a crucial and essential factor of e-commerce. A reliable electronic payment system requires mutual authentication, through which the transacting parties can confirm each other's identity; confidentiality, which ensures that the transaction details are not disclosed to third parties; integrity, which indicates that messages have not been tampered with during transmission; and nonrepudiation, which prevents groundless repudiation of completed transactions. Most consumers use credit or check cards when purchasing items via e-commerce. In such cases, a payment gateway (PG) is used to ensure integrity and nonrepudiation of card payments. This inevitably generates transaction fees as intermediary entities such as PG or value-added network companies intervene in the payment process. Such fees were not a serious issue in the past, as credit card payments were relatively larger in amount and smaller in number of transactions. However, the increasing distribution of credit card terminals, changes in tax deduction rates, more value-added services offered by credit card companies, and rising number of convenience stores processing higher volume of small payments are rapidly generating problems for the e-commerce market, leading consumers and small businesses to raise an issue regarding the fees attached to electronic payment systems. This problem can be addressed using the blockchain technology, as it utilizes component technologies such as hash, asymmetric cryptography algorithm, and public key certificate. Bitcoin, a cryptocurrency using blockchain technology, was made public in a dissertation by Nakamoto (2008). Bitcoin has features such as distributed ledger, consensus algorithm, and mining, but its most important characteristic is decentralization

✉ Seung-Hee Kim
  sh.kim@koreatech.ac.kr

  Shee-Ihn Kim
  eftpos@koreatech.ac.kr

[1] Department of IT Convergence Software Engineering, Korea University of Technology and Education, F411, Engineering Building 1, 1600, Chungjeol-ro, Byeongcheon-myen, Dongnam-gu, Cheonan-si, Chungcheongnam-do 31253, Republic of Korea

in which authority and incentive are made public. Encouraged by such decentralized peer-to-peer (P2P) structure of cryptocurrency, Buterin (2014) developed Ethereum, raising capital through a process called initial coin offering (ICO: similar to initial public offering in stock markets). Ethereum is considered a second-generation blockchain cryptocurrency, owing to its expanded smart contract feature. The success of Bitcoin and Ethereum catalyzed the burgeoning development of numerous altcoin systems. Authentication of identity requires a public key certificate structured with public key infrastructure (PKI), besides security technologies such as one-time password (OTP), smart card, and short message service. Meanwhile, blockchain systems are inherently endowed with public key, private key, and digital signature features, which provide their users integrity and nonrepudiation of payment transactions without having to implement external security measures. The current study intends to propose an electronic payment platform based on the core elements of blockchain technology, i.e., public key, private key, and digital signature. The proposed system is different from the conventional blockchain e-commerce system used by transaction intermediaries. The blockchain system features a decentralized authentication on a ledger that contains agreements and transactions between participating nodes through the blockchain cryptocurrency system. This simplifies the system structure and eliminates the need for external feature modules, thus reducing the overall system development and operating costs and resulting in less fees for merchants. The main implications of this study are summarized as follows.

■The blockchain system can execute a decentralized authentication on a ledger that contains agreements and transactions between participating nodes through the blockchain cryptocurrency system.

■ A blockchain payment technology is developed that ensures transaction integrity and nonrepudiation of transactions between participating nodes.

Section 2 explores the major technologies and investigates the prior research related to the study. Section 3 proposes a model for a payment system using blockchain technology without a PG. Section 4 includes a simple prototype software developed to verify the model's feasibility through actual tests. Finally, Sect. 5 concludes this study.

2 Related work

### 2.1 Background

2.1.1 Blockchain

Bitcoin, released in 2008, is the first blockchain cryptocurrency. It uses a P2P network to enable users to send money to other users online. Because proof-of-work a consensus algorithm, consumes considerable computational power, the system rewards miners with coins, whose payments are maintained in a transaction log. Meanwhile, Ethereum has smart contract features, where the transaction log records script codes and payments are automatically processed when certain conditions are met. In addition, Ethereum has a concept of gas fee, which is used to reward users for authenticating transactions and processing payments. As such, users can enter and utilize the Ethereum platform as long as they pay the gas fee. MultiChain is a private blockchain that is different from Bitcoin and Ethereum, and was made public in a white paper by Greenspan (2015). Its consensus algorithm is a modified version of practical byzantine fault tolerance (PBFT), with characteristics such as improved speed, segmented user authority, and multiasset. It was also selected as the blockchain module for SAP in 2018. Yuan and Wang (2018) asserted that such blockchain cryptocurrency systems comprise three processes: issuance, circulation, and market. The authors argued that such components form an ecosystem. Issuance refers to system implementation and mining of tokens; circulation corresponds to face-to-face and e-commerce transactions; and market refers to the cryptocurrency exchange. The model proposed in the current study utilizes MultiChain, a Bitcoin-based system with improved features and convenience.

2.1.2 Authentication

The prevalence of smartphones is increasing the number of payment transactions processed via mobile devices. QR codes defined in international standards are used to enter an ID or key value during smartphone e-commerce transactions, because they can contain more data than bar codes (ISO/IEC 18004 2006). Because security is becoming more crucial in smartphone payments, Purnomo et al. (2016) proposed a mutual authentication method in which customers and merchants use encrypted QR codes to process payments. Here, a third-party entity is designated to manage PKI certificates and the merchant encrypts the payment information using a public key provided by this third party. The customer requests a private key from the third party, receives payment information from the merchant, and decrypts the information using the private key to authenticate the payment information. This is a decent way to process authentication between merchants and customers, but requires a key pair to be generated for each transaction, with a private key being sent to the customer via the third party. As shown in Fig. 1, in general, the authentication process between the sender and receiver is as follows. The sender hashes the message. The sender's private key is used to encrypt the hashed result to generate a message authentication code (MAC). The sender then transmits the message and MAC to the receiver. The receiver

Fig. 1 Message authentication diagram

MAC : Message Authentication Code
== : Message is authentic and integrity is checked
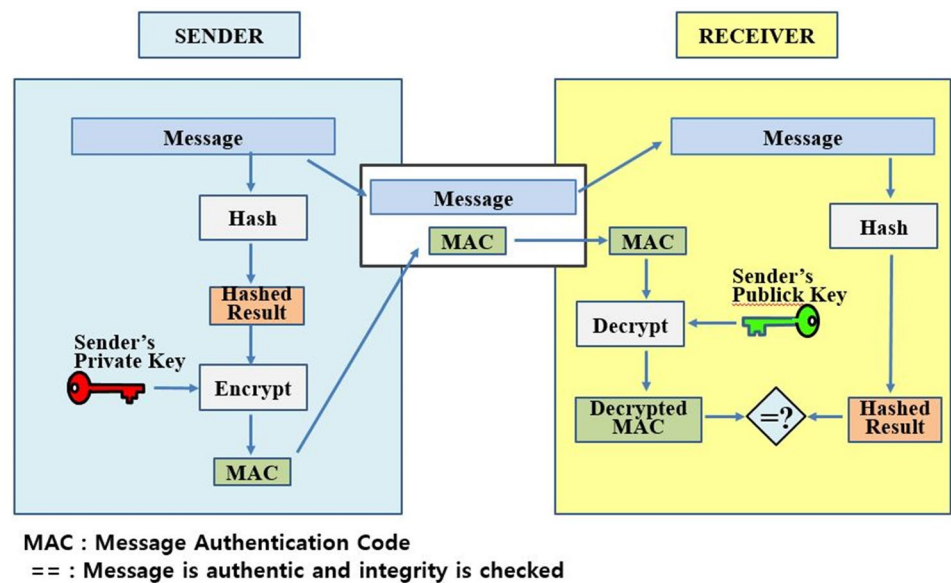
hashes the transmitted message to generate a hashed result and decrypts the received MAC with the sender's public key to generate a decrypted MAC. Finally, the hashed result and decrypted MAC are compared, and if the two have the same value, the integrity of the message and nonrepudiation of the sender are proved. Here, the process executed by the sender is called sign message and that by the receiver is called verify message. The current study uses an authentication method involving these two processes.

2.2 Related work

2.2.1 E-commerce payment

Owing to the prevalence of smartphones, hardware OTP devices have been transposed into smartphone applications. Malik et al. (2014) developed a process in which QR codes are used to operate an OTP smartphone application to enhance the ease of user input. According to Miglicco (2018), companies with business ties in the EU must comply with the General Data Protection Regulation (GDPR) to protect personal information. Violation of the regulation can incur a fine of as much as 20 million Euros or 4% of the company's annual revenue. Kim and Kim (2011) implemented Kerberos by MIT in a new secure credit card payment system. In this model, the distribution of secret keys is achieved with tickets, which are categorized into session tokens and payment tokens. The latter is limited to one-time use, to enhance the system security. Isaaca and Zeadally (2012) indicated that the customer and merchant cannot directly communicate when processing credit card payments on mobile devices, and proposed that PGs should

mediate transactions while using the symmetric-key operation to enhance the processing speed. This method has a higher level of security than conventional models, but it is problematic because of the complexity of key distribution and processing. There have also been continued attempts to replace fiat money with blockchain cryptocurrencies in real-world transactions. Bamert et al. (2013) devised a system in which a snack-vending machine accepts Bitcoins to dispense products. Eskandari et al. (2016) developed a point-of-sale website system that accepts Bitcoin, instead of fiat money, to enable Aunja Cafe in Montreal, Canada, to accept Bitcoins. Meanwhile, Manzoor et al. (2018) implemented an application (dubbed payment gateway) for merchants, which can enable them to accept payments in Ethereum. In this system, merchants can see the increase in their balance, to confirm payments. While there are studies with the objective of implementing blockchain cryptocurrencies in real-world situations, as shown above, e-commerce payment transaction authentication methods that do not require a PG have not been researched.

2.2.2 PG

As shown in Fig. 2, PG is an intermediary system that authorizes e-commerce payments. PGs exist between the merchant and the bank (or card issuer), acting as the middleware.

With the increasing prevalence of online shopping malls, the improvement in credit card payment systems on e-commerce platforms has been extensively studied. A secure connection is set up after the server certificate is authenticated in the PKI authentication system, which
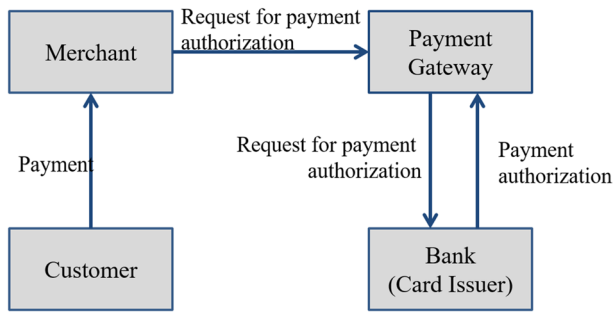
Fig. 2 Typical credit card payment model

Fig. 3 Authentication structure

enables secure e-commerce activities. Zhiwei et al. (2015) improved this system by reducing the certificate authentication time using the certificate path trust index. Meanwhile, Hassan et al. (2018) devised a user-server mutual authentication method by using certificate-less and identity-based public-key cryptography, thereby reducing the burden of authenticating certificates. In addition, OTP feature can be added to e-payment systems to enhance their level of security (Shin 2015), but this puts additional processing burden on such systems. Cheong et al. (2012) proposed a more innovative, efficient, and secure credit card payment system that does not require a PG. However, this model is too complex, as it requires the implementation of security, key, communication, information, payment, and host system modules, each on merchant, customer, and bank (card issuer) systems.

2.2.3 Payment model

To enable a convenient e-commerce payment system without a PG, a separate certificate, OTP, or additional features must be implemented as a module. Blockchain technology, however, is inherently equipped with public key, private key, and digital signature features, which enable the development of a convenient e-commerce payment system without a PG. The current paper proposes the use of blockchain technology to build a model that does not require implementation of external feature modules. Although it is simple in structure and does not require external feature modules, it guarantees integrity and non-repudiation of transaction between the merchant and customer and between the customer and blockchain system, thus reducing the overall system development and operating cost and fees that the customers and merchants have to pay.
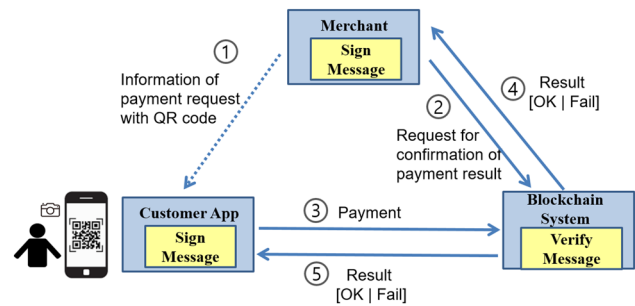
As mentioned above, a payment model using the blockchain technology without a PG has not been researched yet.

Therefore, this study demonstrates the technical feasibility of the proposed model by designing a detailed payment model using blockchain and implementing and demonstrating the prototype software.

3 Model of e-commerce payment system using blockchain without PG

3.1 System structure

The proposed blockchain e-commerce payment system comprises the merchant, customer's smartphone application, and blockchain system. Figure 3 shows the overall system structure, and the payment processing procedure is as follows:

(1) After selling its products and services, the merchant requests the customer to make payment using a blockchain cryptocurrency. This process is indicated with a dotted line because the merchant makes the payment request through a QR code displayed on the customer's web browser, rather than a separate online channel. By contrast, requests indicated with (2), (3), (4), and (5) are all represented with solid lines as they use separate telecommunication lines.

(2) To confirm whether the customer has made the payment, the merchant requests confirmation to the blockchain system.

(3) After purchasing products and services from the merchant, the customer scans the QR code to pay the price to the merchant. The payment is not transmitted directly to the merchant; a payment request is made to the blockchain system, which contains the transaction ledger.

(4) The blockchain system deducts the payment amount from the customer's account and raises the same amount in the merchant's account. After executing this transfer between the accounts, the blockchain system transmits the results to the merchant. When the merchant confirms that the payment was processed normally, it delivers the purchased product or begins to provide the purchased service to the customer.

(5) The blockchain system also transmits the payment result information to the customer's smartphone application.

This is the procedure through which payment is authenticated in the three components of the merchant, customer's smartphone application, and blockchain system. A digital signature is generated at the merchant device through the sign message process and another digital signature is generated on the customer's smartphone application using the sign message function. The digital signatures of the merchant and the customer are verified in the blockchain system, using the verify message function. Figure 4 shows the digital signature and verification procedures in the payment process. The parameters transmitted among the merchant, customer's smartphone application, and the blockchain system are address, amount, transaction time, transaction ID, the merchant's digital signature, and the customer's digital signature. The merchant and customer each have their own public and private keys.

Figure 5 displays a block diagram of the subsystems for the merchant, customer, and blockchain, which are the principals of the blockchain authentication process. The merchant subsystem configures a message containing the merchant's address, amount, transaction time, and transaction ID. The message is signed with the merchant's private key to generate a digital signature, which is displayed as a
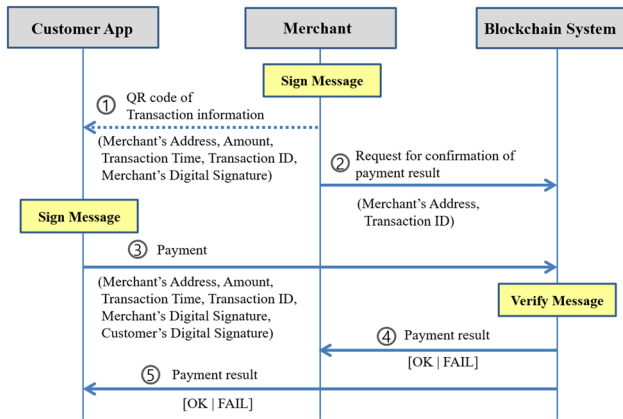

Fig. 4 Blockchain E-commerce payment system architecture
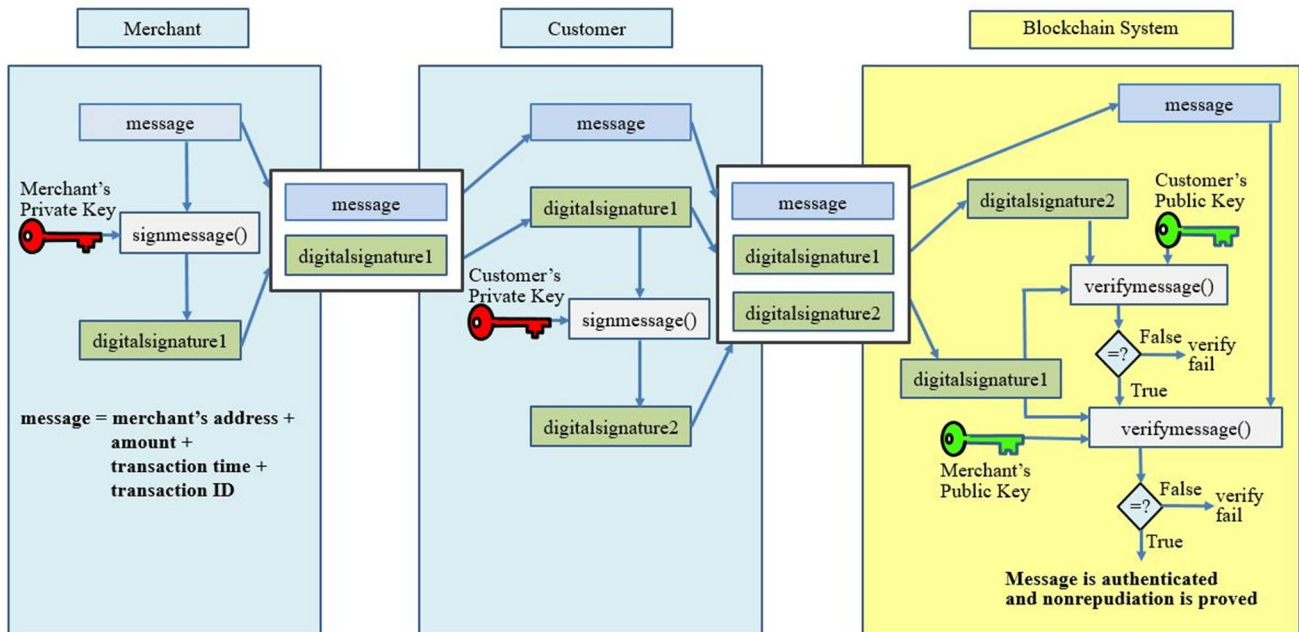

Fig. 5 Block diagram of blockchain authentication subsystems

QR code, including the five parameters on the merchant's online shopping mall screen. Using the QR code, the customer obtains the message and merchant's digital signature (digitalsignature1). The obtained digitalsignature1 is then signed with the customer's private key to generate the customer's digital signature (digitalsignature2). Then, the customer transmits to the blockchain system the message and digitalsignature1 sent by the merchant and digitalsignature2 generated by the customer. Finally, the blockchain system receives the message (containing the merchant's address, amount, transaction time, and transaction ID), digitalsignature1, and digitalsignature2 from the customer. Next, the customer's public key is used to verify digitalsignature1 and digitalsignature2. When the results match, it is proven that digitalsignature1 has integrity and that the customer is the only person who could have sent it. Later, the merchant's public key is used to verify digitalsignature1 and the message (containing the merchant's address, amount, transaction time, and transaction ID). When the results match, it is proven that the message has integrity and that the merchant is the only person who could have sent it. The integrity and nonrepudiation of the payment transaction are guaranteed through this verification process.

3.2 Merchant subsystem

Figure 6 and Table 1 show the data packet delivered from the merchant to the customer using a QR code displayed on the online shopping mall screen. Then, the customer indicates the intention to purchase and the merchant generates a message by connecting its address, transaction time, and transaction ID values in a string. Later, the message is digitally signed with the merchant's private key, generating digitalsignature1. Then, the merchant displays M_Address, Amount, TimeStamp, M_TX_ID, and DigitalSignature1 as a QR code on its online shopping mall screen.

The merchant generates a message with a string of M_Address, Amount, TimeStamp, and M_TX_ID. The configured message is digitally signed with the merchant's address (public key) to generate digitalsignature1. The following is the algorithm for the merchant's digital signature:

Table 1 Merchant's digital signature and message component

Item	Size	Description
M_Address	38 bytes	Merchant's address (public key)
Amount	String	Payment amount
TimeStamp	29 bytes	Payment transaction time (UTC)
M_TX_ID	7 bytes	Merchant's transaction ID
DigitalSignature1	88 bytes	Generated by digitally signing the message with the merchant's private key

---

Algorithm 1 Digital Signature by Merchant
1. message = M_Address + Amount + TimeStamp + M_TX_ID
2. DigitalSignature1 = signmessage(M_Address, message)

In Fig. 6, signmessage() and verifymessage() are functions that process the digital signature. The function signmessage() should principally use a private key, but a public key may be used for convenience. In fact, the use of a public key is recommended for security reasons, as doing so prevents the private key from being exposed in the program source. When the public key is entered in place of the private key, the function internally replaces it with a private key for encryption. Meanwhile, verifymessage() has input parameters of address (public key), digital signature, and message. If the decrypted digital signature and the message have the same value, "true" is returned; otherwise, "false" is returned. DigitalSignature1 is a parameter in which the merchant digitally signs the message containing the string M_Address, Amount, TimeStamp, and M_TX_ID, using its private key. Figure 7 shows the QR code screen containing the five parameter data points as shown in Table 2.

In addition, the QR code is configured with JSON format, as shown in Table 3.
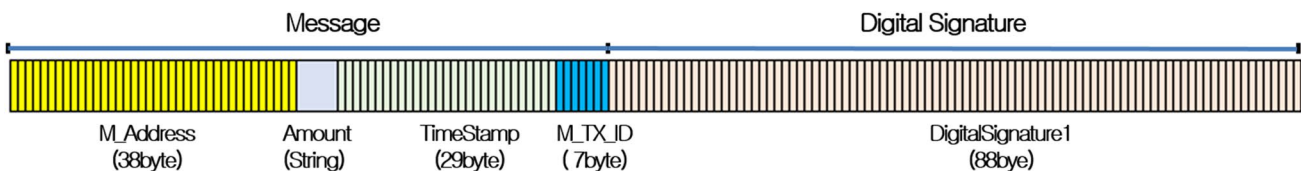

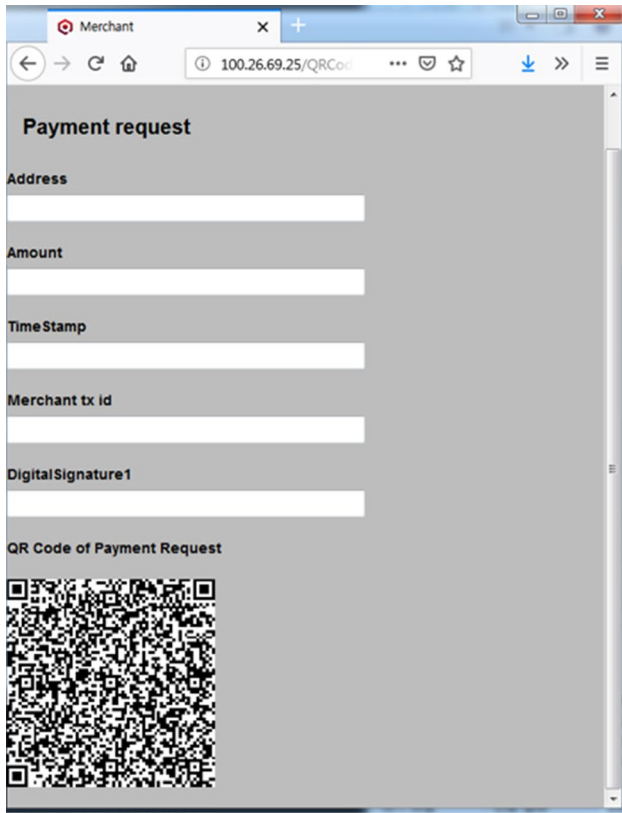**Fig. 6** Format of Merchant's message and digital signature

Fig.7 Merchant screen

3.3 Customer application subsystem

The customer smartphone application is based on the Android operating system. It is used on the merchant's online shopping mall to purchase products and services with blockchain cryptocurrencies. When the customer launches the application and selects the button "QR Code Scan," the phone camera is launched to scan the merchant's QR code on the App, as shown in Fig. 8. After the customer application parses the parameters in the QR code into the JSON format shown in Table 3, M_Address, Amount, TimeStamp, M_TX_ID, and DigitalSignature1

values are obtained by the customer. As shown in Fig. 9 and Table 4, the customer application generates Digital-Signature2 to prove integrity and nonrepudiation.

That is, digitalsignature1 generated by the merchant is digitally signed again with the customer's private key to generate digitalsignauture2. The customer's address (C_Address), an input parameter, is a public key, which is replaced by a private key in the signmessage() function. The customer application has its own address (public key) and a private key. Algorithm 2 is the digital signature algorithm of the customer application as shown in Table 5.

Algorithm 2 Digital Signature by Customer App
INPUT : DigigitalSignature1
1. DigitalSignature2 = signmessage(C_Address, DigitalSignature1)

The customer selects "Payment" button in the customer application, as shown in Fig. 8, to make correct payment to the merchant. Here, the customer application transmits to the blockchain system M_Address, Amount, TimeStamp, M_TX_ID, and DigitalSignature1 obtained by the merchant's QR code and the generated DigitalSignature2, as shown in Fig. 9.

Table 3 QR code formatted with JSON

```
{
"address": merchant's address (public key),
"amount": transaction amount,
"timestamp": time of transaction (UTC format),
"m_tx_id": merchant's transaction unique number,
"digitalsignature1": digital signature from
signmessage(merchant's address, message) function
}
```

Table 2 signmessage() and verifymessage() functions

Function	Return value	Description
signmessage()	Digital signature	Returns a digital signature, which proves that the message was approved by the owner of the address or private key
		DigitalSignature = signmessage([address | private key], message)
verifymessage()	True or false	Verifies that message was approved by the owner of address by checking the digital signature. The result is true or false unless an error occurs
		[True | False] = verifymessage(address, digitalsignature, message)

Fig. 8 Customer application screen

3.4 Blockchain subsystem

The blockchain system receives a request to confirm payment from the merchant, as shown in Fig. 3-(2). Meanwhile, Figs. 3 and 4-(3) show the payment information received from the customer application. As indicated by the design described above, the payment information comprises M_address, Amount, TimeStamp, M_TX_ID, digitalsignature1, and digitalsignature2. As shown in Fig. 10, the blockchain system executes a two-step message authentication process. The first step is to execute the verification function for the customer, followed by the same process for the merchant in the next step. When the message verification result is "true," it is proven that the messages transmitted by the customer and merchant have integrity and that the two parties are the only people who could have sent the messages, which ensures nonrepudiation.

Table 4 Digital signature processed by the customer application

Item	Size	Description
M_Address	38 bytes	Get value from QR code
Amount	String	Get value from QR code
TimeStamp	29 bytes	Get value from QR code
M_TX_ID	7 bytes	Get value from QR code
DigitalSignature1	88 bytes	Get value from QR code
DigitalSignature2	88 bytes	Generated by digitally signing DigitalSignature1 with the customer's private key

Table 5 Hardware and software configurations for the experiment

Component	Hardware	Software
Merchant	AWS EC2 (m5.large)	Node.js v8.12.0
Customer application	LG G Pad HomeBoy	Android 4.2.2, Android Studio 3.2.1, Java SDK version 28
Blockchain system	AWS EC2 (m5.large)	Node.js, MultiChain 1.0.3

Algorithm 3 Authentication by Blockchain System

INPUT : M_Address, Amount, TimeStamp, M_TX_ID, DigitalSignature1, DigitalSignature2 from Customer App,

       M_Address, M_TX_ID from Merchant

1.   message = M_Address + Amount + TimeStamp + M_TX_ID
2.   // Step 1 : Customer authentication
3.   if (verifymessage(C_Address, DigitalSignature2, DigitalSignature1)) {
4.   // Step 2 : Merchant authentication
5.   if (verifymessage(M_Address, DigitalSignature1, message)) {
6.   if (M_Address + M_TX_ID from Merchant ==
7.   M_Address + M_TX_ID from Customer App) {
8.   send OK to Customer App and Merchant
9.   } else {
10.   send FAIL to Customer App and Merchant
11.   }
12.   } else {
13.   send FAIL to Customer App and Merchant
14.   }
15.   } else {
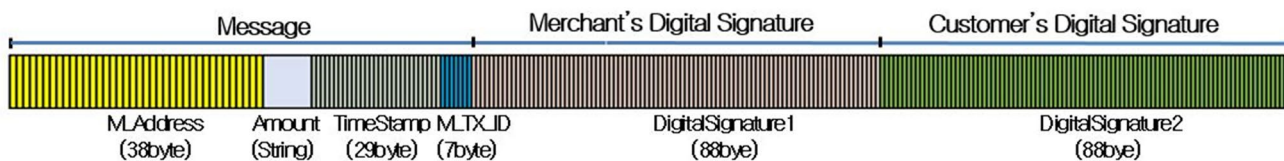16.   send FAIL to Customer App and Merchant
17.   }

Fig. 9 Data format of message and digital signature processed by the customer application
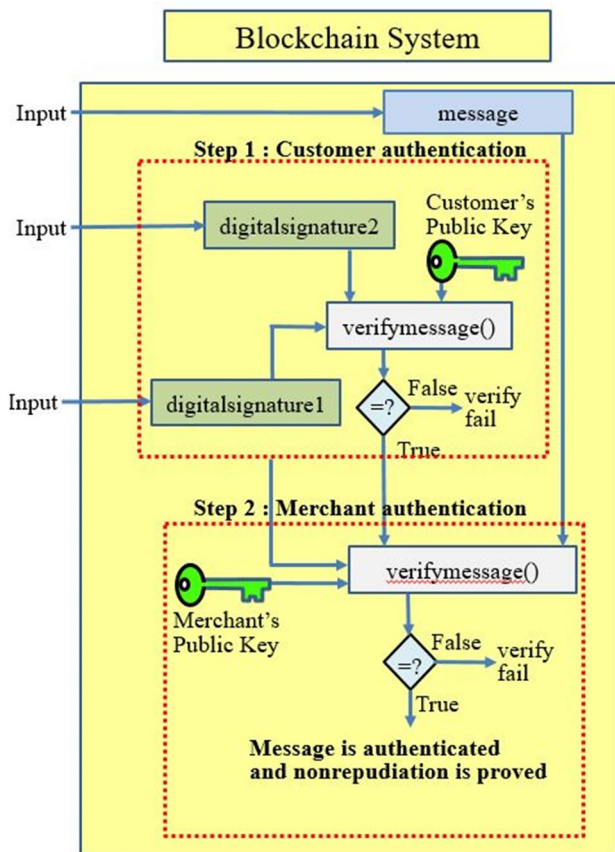

Fig. 10 Two-step message authentication process of the blockchain subsystem

Step 1 is a procedure that authenticates integrity and nonrepudiation of the payment request information from the customer application. Here, digitalsignature2, which was signed by the customer application, is verified using the function verifymessage(). That is, verifymessage() decrypts digitalsignature2 using the customer's public key and compares the resulting value with that of digitalsignature1. When the values match, the system returns "true." In Step 2, the integrity and nonrepudiation of the merchant's payment request information are authenticated. The digitalsignature1 signed by the merchant is verified using the

function verifymessage(). That is, verifymessage() decrypts digitalsignature1 using the merchant's public key and compares the resulting value with that of the message. When the values match, the system returns "true." In this case, the message comprises M_address, Amount, TimeStamp, and M_TX_ID. When the two steps of message authentication are successfully executed, M_TX_ID of the merchant is compared to transmit the payment result. Additionally, the value of timestamp and the current time in the blockchain system can be compared to block replay attacks. Algorithm 3 shows the message authentication procedure described above.

4 Experiments

The current study implemented the e-commerce blockchain payment authentication system to validate the proposed model and algorithms. Figure 11 shows the experiment environment in which the authentication results for the merchant, customer, and blockchain subsystems are verified.

4.1 Experiment environment

The Amazon Web Services (AWS), an Amazon cloud service, was used to set up the environment to verify the merchant and blockchain subsystems. The size of the generated instance was m5.large for EC2. The operating system was RedHat, and the software development language was node.js. The hardware containing the customer application was LG G Pad, whose operating system was Android and the software development language was Android java. The blockchain system used MultiChain, an open-source software for blockchain cryptocurrencies.

4.2 Experimental results

The overall experiment scenario is as follows: First, when the customer selects a product on the merchant's online shopping mall, the payment screen shown in Fig. 12 is generated. The customer scans the QR code to execute the payment procedure. The blockchain subsystem transmits the payment result to the merchant and the customer. To verify
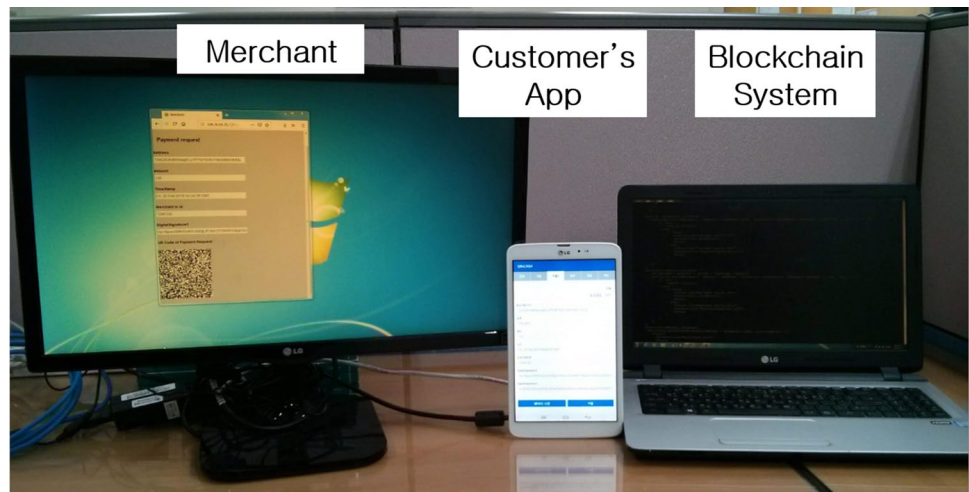
the accuracy of the features, tests were run sequentially on the merchant, customer, and blockchain subsystems. The verification process confirmed whether the digital signature for the merchant's message, as well as that for the customer's message, was accurately created. In addition, the accuracy of digital signatures of the merchant and customer was verified in the blockchain system.
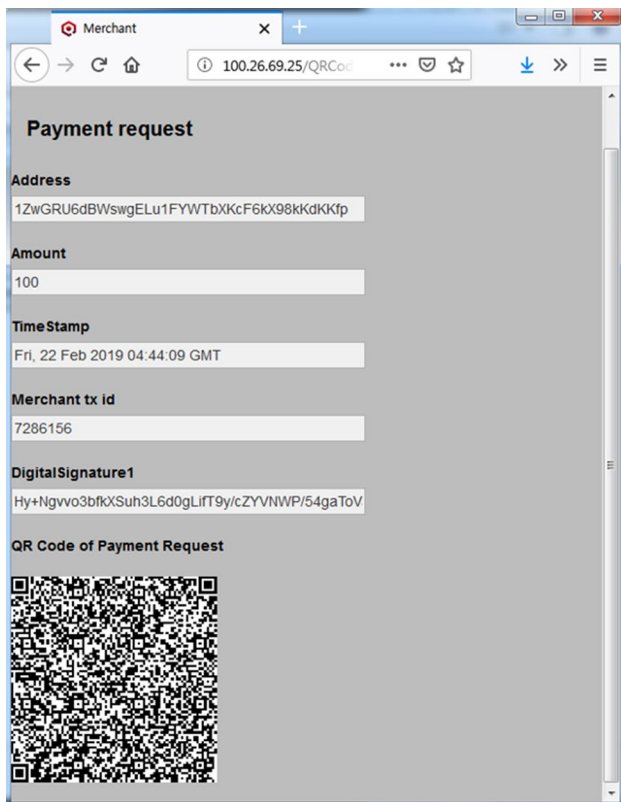
4.2.1 Merchant

Table 6 shows the data format of the QR code that includes information of digitalsignature1, and the value resulting from the merchant digitally signing the message "address = 1ZwGRU6dBWswgELu1FYWTbXKcF6kX98k-KdKKfp, amount = 100, timestamp = Fri, 22 Feb 2019 14:44:09 GMT, m_tx_id = 7286156" using the merchant's address.

To process the customer's convenient payment, the merchant's online shopping mall displays a QR code containing the parameters of digitalsignature1 and M_Address, Amount, TimeStamp, and M_TX_ID, as shown in Fig. 12.

4.2.2 Customer application

The customer uses the customer application to purchase a product or a service in the merchant's online shopping mall. The customer selects the "QR Code Scan" button to scan the QR code on the online shopping mall screen, as shown in Fig. 13. The QR code is scanned and parsed to obtain the values of M_address, Amount, TimeStamp, M_TX_ID, and digitalsignature1. In addition, when the customer selects

Fig. 12 QR code on the merchant's screen

Table 6 JSON format data of QR code information

```
{
"address":"1ZwGRU6dBWswgELu1FYWTbXKcF6
kX98kKdKKfp",
"amount":"100",
"timestamp":"Fri, 22 Feb 2019 14:44:09 GMT",
"m_tx_id":"7286156",
"digitalsignature1":"Hy+Ngvvo3bfkXSuh3L6d0gLif
T9y/cZYVNWP/54gaToVapQu1vRSm1QvdtwNHw
5LuBCkLz1rchH3mfh+rUb4UAg="
}
```

"Payment" button, as shown in Table 7, the application generates digitalsignature2 by running digitalsignature1 in the signmessage() function and the customer's private key. Later, the customer application transmits the parameters of M_Address, Amount, TimeStamp, M_TX_ID, digitalsignature1, and digitalsignature2 to the blockchain system.

Table 8 shows the data format in the payment information sent by the customer to the blockchain system.

Fig. 13 QR code scan screen in the customer application

4.2.3 Blockchain system

The customer's address is "1BisEwmwfLKBkoqox-T1NNUeJ2HbWdqmJyMFyGL." The value of the message received from the customer application is the merchant's address = "1ZwGRU6dBWswgELu1FYWTbXKcF6kX98k-KdKKfp," amount = "100," timestamp = "Fri, 22 Feb 2019 14:44:09 GMT," ditialsignature1 = " Hy + Ngvvo3bfkX-Suh3L6d0gLifT9y/cZYVNWP/54gaToVapQu1vRSm1Q vdtwNHw5LuBCkLz1rchH3mfh + rUb4UAg = ," digitalsignature2 = ":" ICsWAZLREsxiq9hNk/dFtpdfEBXtpOjP-wKAsbWlIQ5/wdp2DKfdSWPPSb7F85yTOYa9zsTrSX/ TDsXKMMc4qRYg = ." The values of the received message, digitalsignature1, and digitalsignature2 are verified using the function verifymessage(). That is, digitalsignature2 is decrypted using the customer's public key and compared with digitalsignature1. When the values are the same, it is proven that the message sent by the customer has integrity, with a guarantee that only the customer could have sent it. Then, the screen displays the sentence "Customer authentication is OK." Later, digitalsignature1 is decrypted using the merchant's public key and compared with the message (merchant's address, amount, timestamp, m_tx_id). If the values are the same, it is proven that the message sent by the merchant has integrity, with a guarantee that only the merchant could have sent it. Then, the screen displays the sentence "Merchant authentication is OK." In addition, as shown in Fig. 14, the start time of the authentication is displayed as "Start Time:," the end time is displayed as "End Time:," and the duration is indicated as "Duration Time:." Consequently, the message authentication processing time was 10 ms (100 TPS). According to a publication by VISANet, the average throughput of VISA is approximately 1700 TPS, and according to PayPal's publication, Paypal's average throughput is approximately 290 TPS (VISANet 2013; Paypal 2018). Considering the CPU clock speed in the environment of the current experiment and the clock speeds of the hardware servers used in the industry, a speed of 100 TPS is outstanding. Moreover, the TPS performance can be easily enhanced by expanding the cloud instance size or multithreading programs that process the authentication requests.

Table 7 Data in the QR code and digitalsignature2	Item	Size	Description	Comment
	M_Address	38 bytes	Obtained from the QR code	MultiChain spec
	Amount	String	Obtained from the QR code	node.js data format
	TimeStamp	29 bytes	Obtained from the QR code	node.js data format
	M_TX_ID	7 bytes	Obtained from the QR code	node.js data format
	digitalsignature1	88 bytes	Obtained from the QR code	MultiChain spec
	digitalsignature2	88 bytes	Generated with signmessage(customer's address, digitalsignature1) function	MultiChain spec

Table 8 Customer payment information in JSON format

```
{
    "address":"1ZwGRU6dBWswgELu1FYWTbXKc
F6kX98kKdKKfp",
    "amount":"100",
    "timestamp":"Fri, 22 Feb 2019 14:44:09 GMT",
    "m_tx_id":"7286156",
    "digitalsignature1":"Hy+Ngvvo3bfkXSuh3L6d0g
LifT9y/cZYVNWP/54gaToVapQu1vRSm1QvdtwN
Hw5LuBCkLz1rchH3mfh+rUb4UAg=",
    "digitalsignature2":"ICsWAZLREsxiq9hNk/dFtpdf
EBXtpOjPwKAsbWlIQ5/wdp2DKfdSWPPSb7F85y
TOYa9zsTrSX/TDsXKMMc4qRYg= "
}
```

Fig. 14 Authentication success message and duration

5 Conclusion

When processing a credit card payment in e-commerce settings, customers and merchants are required to use a PG service. The current paper proposed a convenient payment model without a transaction intermediary, such as public key certificate or PG, and implemented a design to confirm its application potential. An experiment was conducted to verify that the internal blockchain features, such as public key, private key, and digital signature, can be used to construct a functioning electronic payment system without having to implement additional modules. In conclusion, it was confirmed that a system in which the merchant, customer, and blockchain subsystems, each executing authentication, can guarantee integrity and nonrepudiation of payment transactions. The authentication performance was reasonable, at 100 TPS. The proposal set forth in the current study makes data transmission between merchants and customers easier and more convenient by using the QR code, and as such, may serve as an alternative for resolving issues surrounding payment fees for processing e-commerce transactions. However, there is a risk in which the blockchain system's public-distributed transaction ledger system may lead to disclosure of personal identification data, which in turn may enable

malicious users to combine such data to identify individuals using the system. In addition, this system requires a design for multithreading system architecture if the system is to process several payment transactions. Despite such weaknesses, our proposed model will propel crucial technical developments in e-commerce payment systems and ensure competitive advantage of e-commerce systems, because e-commerce is becoming more prevalent and uses of blockchain cryptocurrencies are becoming more diverse, besides ICOs.

References

Bamert T, Decker C, Elsen L, Wattenhofer R, Welten S (2013) Have a snack, pay with Bitcoins in peer-to-peer computing (P2P). IEEE thirteenth international conference on IEEE 2013, pp 1-5

Buterin V (2014) Ethereum white paper: a next-generation smart contract and decentralized application platform. https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf. Accessed 28 Feb 2019

Cheong C, Fong S, Lei P, Chatwin C, Young R (2012) Designing an efficient and secure credit card-based payment system with web services based on the ANSI X9.59-2006. J Inf Process Syst 8(3):495–520

Eskandari S, Clark J, Hamou-Lhadj A (2016) Buy your coffee with Bitcoin: real-world deployment of a Bitcoin point of sale terminal. 2016 Intl IEEE conferences on ubiquitous intelligence and computing, advanced and trusted computing, scalable computing and communications, cloud and big data computing, internet of people, and smart world congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), IEEE, pp 382–389. https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0073

Greenspan G (2015) MultiChain private blockchain—white paper. https://www.multichain.com/download/MultiChain-White-Paper.pdf. Accessed 28 Feb 2019

Hassan A, Eltayieb N, Elhabob R, Li F (2018) An efficient certificateless user authentication and key exchange protocol for client-server environment. J Ambient Intell Hum Comput 9:1713–1727

International standard ISO/IEC 18004, Information technology—automatic identification and data capture techniques—QR Code 2005 bar code symbology specification. ISO/IEC 18004:2006(E), Second edition

Isaaca J, Zeadally S (2012) Anonymous secure payment protocol in a payment gateway centric model. Procedia Comput Sci 10:758–765

Kim J, Kim Y (2011) A secure credit card transaction method based on Kerberos. J Comput Sci Eng 5(1):51–70

Malik J, Girdhar D, Dahiya R, Sainarayanan G (2014) Multifactor authentication using a QR code and a one-time password. J Inf Process Syst 10(3):483–490

Manzoor A, Hu Y, Liyanage M, Ekparinya P, Thilakarathna K, Jourjon G, Seneviratne A, Kanhere S, Ylianttila M (2018) Demo: a delay-tolerant payment scheme based on the Ethereumblockchain. https://arxiv.org/abs/1801.10295

Miglicco G (2018) GDPR is here and it is time to get serious. Comput Fraud Secur 2018(9):9–12

Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. Accessed 28 Feb 2019

PayPal (2018) PayPal reports second quarter 2018 results. https://investor.paypal-corp.com/news-releases/news-release-details/paypal-reports-second-quarter-2018-results?ReleaseID=1072972. Accessed 28 Feb 2019

Purnomo A, Gondokaryono Y, Kim C (2016) Mutual authentication in securing mobile payment system using encrypted QR code based on public key infrastructure. 2016 IEEE 6th international conference on system engineering and technology(ICSET), October 3–4, 2016 Bandung, Indonesia

Shin K (2015) E-payment authentication system using QR code and mobile OTP. J Korean Inst InfTechnol 13(7):75–82

Thompson F, Tuzovic S, Braun C (2019) Trustmarks: Strategies for exploiting their full potential in e-commerce. Bus Horiz 62(2):237–247

VisaNet (2013) VisaNet Catalyst for Commerce. https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/VisaNet-Network-Processing-Overview.pdf. Accessed 28 Feb 2019

Yuan Y, Wang FY (2018) Blockchain and cryptocurrencies: model, techniques, and applications. IEEE Trans Syst Man CybernSyst 48(9):1421–1428

Zhiwei G, Yingxin H, Kai L (2015) CPTIAS: a new fast PKI authentication scheme based on certificate path trust index. J Ambient Intell Hum Comput 6:721–731

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.