

SECURE AND COMPLIANT MULTI-CRYPTOCURRENCY PAYMENT GATEWAY**Field**

[0001] The present invention relates generally to cryptocurrency payment gateways.

Background

[0002] Payment gateways allow merchants to accept payments by connecting payment processors with merchant account providers. In some cases, these payment gateways themselves act as the account provider, either by issuing accounts or providing sub accounts linked to the gateway's own merchant account. In the latter, payment gateways bear liabilities related to anti-fraud and anti-money laundering regulations for the processed transactions. With traditional payment methods such as credit card, debit card, stored value wallets (Alipay, WeChatPay, PayPal), payment gateways protect legitimate consumers by performing anti-fraud assessments, throttling payments, and verifying advisory lists, and as a last resort, triggering chargeback processes. Similarly, to protect merchants, features such as anti-fraud assessments, 3DS verifications, and charge-back guarantees are offered as value added services, when processing payments. However, with current facilities that are available in the market, it is not possible to perform anti-fraud and anti-money laundering assessments when processing cryptocurrency payments due to the anonymous nature of such transactions.

[0003] Cryptocurrency is on the verge of getting broad acceptance as a form of payment for products and services. However, existing solutions for processing cryptocurrency payments for e-commerce transactions suffer from several drawbacks.

[0004] For example, current mechanisms that allow merchants accept cryptocurrency as payment for goods and services rely on merchants directly integrating with cryptocurrency exchanges on a one-to-one relationship basis. Such mechanisms do not offer credit card, debit card or store value wallets as alternative payment options. It is therefore difficult for merchants to offer cryptocurrency as an integrated payment option, alongside other payment methods, to consumers. In such an environment, merchants must develop their own integrated hosted payment page/component, and it may not be possible for all

transactions performed on the merchant's e-commerce site to be settled into a single acquiring fiat account.

[0005] Another drawback with currently available solutions, is that the way merchants integrate with cryptocurrency exchanges are different from the way they integrate with payment gateways to accept payments with credit card, debit card or store value wallets. Previously proposed solutions relied on a progressive web application being developed by the merchant that requires consumers to have a mobile application which converts cryptocurrency to fiat currency, and then processes the payment through payment card rails.

[0006] When performing fraud assessments on payments with cryptocurrencies, current technologies do not consider a risk mitigation approach. They do not consider the source of the fiat funds used to obtain the cryptocurrency or the contents of the relevant shopping basket to determine high risk transactions. One proposed approach attempts to prevent fraudulent transactions from being accepted to a blockchain by inspecting all the transactions of a block to identify those mined by a fraudulent entity. Another proposed solution proposes an approach where cryptocurrency wallets are linked to fiat currency wallets, and aggregate user profiles are held in an exchange by linking the wallets. Then, AML (Anti Money Laundering) and anti-fraud assessments are performed based on the aggregate user profile. However, implementation of such a mechanism is not possible with current mainstream cryptocurrencies such as Bitcoin, Ethereum, Litecoin, XRP, etc.

[0007] In view of this background, there is a need for a secure and compliant multi-cryptocurrency payment gateway.

[0008] It is a preferred object of embodiments of the present invention to at least partially address or ameliorate one or more of the above disadvantages, or at least provide a useful alternative.

Summary

[0009] According to the present invention, there is provided a system, comprising:
a memory; and
a processor configured by instructions stored in the memory to:

receive, at a payment gateway, a payment request and shopping basket details of a customer from a merchant, wherein the payment request comprises a request for the payment gateway to pay a fiat currency amount to the merchant after an equivalent cryptocurrency amount has been transferred from a cryptocurrency wallet of the customer to a cryptocurrency wallet of the payment gateway;

generate a token representing the payment request;

store the token and the shopping basket details for subsequent processing of the payment request by the payment gateway;

provide an interface to the customer to select a cryptocurrency exchange to transfer the equivalent cryptocurrency amount from the cryptocurrency wallet of the customer to the cryptocurrency wallet of the payment gateway;

request the cryptocurrency exchange to sell the equivalent cryptocurrency amount in the cryptocurrency wallet of the payment gateway for the fiat currency amount;

receive a transfer of the fiat currency amount from the cryptocurrency exchange to the payment gateway;

notify the merchant and the customer that the payment request has been successfully processed by the payment gateway;

settle the payment request by transferring the fiat currency amount from the payment gateway to the merchant.

[0010] The interface provided to the customer to select the cryptocurrency exchange may comprise a login uniform resource locator (URL) of the cryptocurrency exchange.

[0011] Alternatively, the interface provided to the customer to select the cryptocurrency exchange may comprise a quick response (QR) payment code for the cryptocurrency exchange.

[0012] Further alternatively, the interface provided to the customer to select the cryptocurrency exchange may comprise a first further token that includes the token representing the payment request, wherein the first further token allows the customer to authorise the cryptocurrency exchange to send the payment gateway a second further token including the first further token that allows the payment gateway to retrieve a balance amount and a transaction history of the cryptocurrency wallet of the customer.

[0013] The payment gateway may perform a risk assessment for the payment request based at least in part on the shopping basket details and the transaction history of the cryptocurrency wallet of the customer.

[0014] If the risk assessment is satisfactory, the payment gateway may use the second further token to request the cryptocurrency exchange to transfer the equivalent cryptocurrency amount from the cryptocurrency wallet of the customer to the cryptocurrency wallet of the payment gateway.

[0015] The payment gateway may generate a non-fungible token (NFT) representing the risk assessment for the payment request.

[0016] The payment gateway may store the NFT in a customer profile of the customer.

[0017] The risk assessment may comprise one or both of an AML risk assessment and a fraud risk assessment.

[0018] The token representing the payment request, and the first and second further tokens, may each comprise an encrypted JSON Web Token (JWT).

[0019] The present invention also provides a method, comprising:

- receiving, at a payment gateway, a payment request and shopping basket details of a customer from a merchant, wherein the payment request comprises a request for the payment gateway to pay a fiat currency amount to the merchant after an equivalent cryptocurrency amount has been transferred from a cryptocurrency wallet of the customer to a cryptocurrency wallet of the payment gateway;

- generating a token representing the payment request;

- storing the token and the shopping basket details for subsequent processing of the payment request by the payment gateway;

- providing an interface to the customer to select a cryptocurrency exchange to transfer the equivalent cryptocurrency amount from the cryptocurrency wallet of the customer to the cryptocurrency wallet of the payment gateway;

- requesting the cryptocurrency exchange to sell the equivalent cryptocurrency amount in the cryptocurrency wallet of the payment gateway for the fiat currency amount;

receiving a transfer of the fiat currency amount from the cryptocurrency exchange to the payment gateway;

notifying the merchant and the customer that the payment request has been successfully processed by the payment gateway;

settling the payment request by transferring the fiat currency amount from the payment gateway to the merchant.

[0020] The present invention also provides a non-transitory machine-readable medium having stored thereon machine-readable instructions executable to cause a machine to perform operations comprising:

receiving, at a payment gateway, a payment request and shopping basket details of a customer from a merchant, wherein the payment request comprises a request for the payment gateway to pay a fiat currency amount to the merchant after an equivalent cryptocurrency amount has been transferred from a cryptocurrency wallet of the customer to a cryptocurrency wallet of the payment gateway;

generating a token representing the payment request;

storing the token and the shopping basket details for subsequent processing of the payment request by the payment gateway;

providing an interface to the customer to select a cryptocurrency exchange to transfer the equivalent cryptocurrency amount from the cryptocurrency wallet of the customer to the cryptocurrency wallet of the payment gateway;

requesting the cryptocurrency exchange to sell the equivalent cryptocurrency amount in the cryptocurrency wallet of the payment gateway for the fiat currency amount;

receiving a transfer of the fiat currency amount from the cryptocurrency exchange to the payment gateway;

notifying the merchant and the customer that the payment request has been successfully processed by the payment gateway;

settling the payment request by transferring the fiat currency amount from the payment gateway to the merchant.

Brief Description of Drawings

[0021] Embodiments of the invention will now be described by way of example only with reference to the accompanying drawings, in which:

Figure 1 is a flow chart of a method for a secure and compliant multi-cryptocurrency payment gateway according to an embodiment of the present invention;

Figure 2 is an architecture diagram of a computer system for performing the method;

Figures 3 to 9 are user interfaces displayed in a customer browser during the method; and

Figures 10 and 11 are data flow diagrams of example implementations of the method.

Description of Embodiments

[0022] Prior to a description with reference to the drawings, to help understanding of the present invention, terms used in this specification are described in brief.

[0023] Payment gateway: sits in between a consumer and a merchant and ensures that funds are transferred securely and correctly when a transaction is performed. They usually integrate with multiple channels and allow merchants to provide multiple payment options to consumers. When processing credit card payments, these gateways provide value added services such as real-time anti-fraud assessments to minimise a merchant's exposure to fraudulent transactions.

[0024] Cryptocurrency: a form of electronic money created from code using an encrypted string. Ownership of cryptocurrency is usually recorded in a cryptographically encrypted immutable sequence of data blocks called a blockchain. The most popular cryptocurrencies allow owners to maintain anonymity and privacy because ownership is linked to a wallet address which is usually just a cryptographic public key.

[0025] Cryptocurrency exchange: an entity that allows customers to trade cryptocurrencies. They also provide means to trade cryptocurrencies with fiat money (or fiat currencies).

[0026] Public key cryptography: a method by which data is encrypted and decrypted using two different keys: a private key and a public key. The public key is derived from the private key. However, it is not possible to derive the private key from the public key. Public

key cryptography is asymmetric: ie, data encrypted with a public key can only be decrypted with the corresponding private key and vice-versa.

[0027] JWT: an open internet standard used to securely transfer claims (ie, pieces of information) between two parties. These claims are encrypted using public key cryptography, and digitally signed or integrity protected using a message authentication code (MAC). A MAC is a tag which confirms that the message from the stated sender has not been changed.

[0028] Figure 1 is a flow chart of a method 100 for providing a secure and compliant multi-cryptocurrency payment gateway according to an embodiment of the present invention. The method 100 may be implemented as software executing in a computer system 200 illustrated in Figure 2. The computer system 200 may comprise a customer browser 210, merchant web page 220, payment gateway 230, and cryptocurrency exchange 240 communicating with one another over a network.

[0029] The method may start at step 110 by receiving, at the payment gateway 230, a payment request and shopping basket details of a customer 210 from a merchant 220. The payment request may comprise a request for the payment gateway 230 to pay a fiat currency amount to a bank account of the merchant 220 after an equivalent cryptocurrency amount has been transferred from a cryptocurrency wallet of the customer 210 to a cryptocurrency wallet of the payment gateway 230.

[0030] Next, at step 120, a token T1 representing the payment request may be generated by the payment gateway 230. At step 130, the token and the shopping basket details may be stored at the payment gateway 230 for subsequent processing of the payment request by the payment gateway 230.

[0031] At step 140, an interface may be provided to the customer 210 to select a cryptocurrency exchange 240 to transfer the equivalent cryptocurrency amount from the cryptocurrency wallet of the customer 210 to the cryptocurrency wallet of the payment gateway 230.

[0032] At step 150, the payment gateway 230 may request the cryptocurrency exchange 240 to sell the equivalent cryptocurrency amount in the cryptocurrency wallet of the payment gateway 230 for the fiat currency amount.

[0033] A transfer of the fiat currency amount from the cryptocurrency exchange 240 to a bank account of the payment gateway 240 may be received at step 160.

[0034] At step 170, the merchant 220 and the customer 210 may be notified by the payment gateway 230 that the payment request has been successfully processed.

[0035] The method 100 may end at step 180 by settling the payment request by transferring the fiat currency amount from the bank account of the payment gateway 230 to the bank account of the merchant 220. The transfer of the fiat currency amount may be processed by generating a digital credit card that allows the payment gateway 230 to pay the fiat currency amount to the merchant as a regular credit card payment.

[0036] Referring to Figure 5, the interface provided to the customer 210 to select the cryptocurrency exchange 240 may comprise a login URL of the cryptocurrency exchange 240. Alternatively, as shown in Figure 9, the interface provided to the customer 210 to select the cryptocurrency exchange 240 may comprise a QR payment code for the cryptocurrency exchange 240.

[0037] In these embodiments, the cryptocurrency exchange 240 may authenticate the customer 210, and the customer 210 may use the cryptocurrency exchange 240 to process a transfer the equivalent cryptocurrency amount from the cryptocurrency wallet of the customer 210 to the cryptocurrency wallet of the payment gateway 230.

[0038] In alternative embodiments, the payment gateway 230 may perform risk assessments for the payment request. In these embodiments, the interface provided to the customer 210 to select the cryptocurrency exchange 240 may comprise a first further token T2 that includes the token T1 representing the payment request. The first further token T2 may allow the customer 210 to authorise the cryptocurrency exchange 240 to send the payment gateway 230 a second further token T3 that includes the first further token T2 and which allows the payment gateway 230 to retrieve a balance amount and a

transaction history of the cryptocurrency wallet of the customer 230 from the cryptocurrency exchange 240.

[0039] The payment gateway 230 may then perform a risk assessment for the payment request based at least in part on the shopping basket details, and the balance amount and the transaction history of the cryptocurrency wallet of the customer 210. If the risk assessment is satisfactory, the payment gateway 230 may use the second further token T3 to request the cryptocurrency exchange 240 to transfer the equivalent cryptocurrency amount from the cryptocurrency wallet of the customer 210 to the cryptocurrency wallet of the payment gateway 230.

[0040] The payment gateway 230 may generate a non-fungible token (NFT) representing the risk assessment for the payment request. The payment gateway 230 may also store the NFT in a customer profile of the customer 210. The risk assessment performed by the payment gateway 230 may comprise one or both of an AML risk assessment and a fraud risk assessment. The token representing the payment request T1, and the first and second further tokens T2, T3, may each comprise an encrypted JWT.

[0041] The following Examples are intended to illustrate the invention. They are not intended to limit the scope of the invention.

Example 1 – Non-tokenised direct processing at cryptocurrency exchange

[0042] In this example, Figures 3 to 8 are user interface mock-ups displayed in a customer browser 210 showing a user experience using Stellar Lumens as a selected cryptocurrency to pay for a shopping basket on a merchant web page 220.

[0043] Figure 3 shows a hosted payment page which is embedded into the checkout page of a merchant's website 220. Options to select payment with cryptocurrencies are provided. Once a cryptocurrency payment option is selected, a customer 210 may select a cryptocurrency exchange 240 at which their wallet is held. In Figure 4, the cryptocurrency exchange 240 is selected by the customer 210.

[0044] Figure 5 shows that the customer 210 is redirected to a login page at the selected cryptocurrency exchange 240. Once the customer 210 logs in, the list of wallets with

sufficient balances is displayed, and they select the wallet/cryptocurrency, as shown in Figure 6.

[0045] Figure 7 shows conversion rate being presented to the customer 210 for review and authorisation of payment.

[0046] Figure 8 is the payment confirmation page which is shown before the customer 210 is redirected back to the merchant's website 220.

[0047] Figures 10 and 11 are end-to-end data flow diagrams which describe stages of this Example 1 in further detail.

Initialisation of payment process and selection of cryptocurrency exchange

[0048] A customer browser 210 initiates checkout process on a merchant server 220 at step 101. At step 102, the customer 210 select cryptocurrency as the payment method. The merchant website 220 passes shopping basket details to the payment gateway (PG) 230 and requests a first token (T1) to track the end-to-end payment flow.

[0049] The PG 230 generates a token T1 and stores the shopping basket details against that token T1 at step 104. T1 is returned to the merchant website 220 at step 105. The merchant's website 220 in turn passes the T1 to the customer's browser 210. The checkout page uses token T1 to initialise a cryptocurrency payment process and presents the customer 210 with available cryptocurrency exchanges 240. In step 107, the customer 210 selects a cryptocurrency exchange (CE) 240.

Authentication of customer and granting access to crypto payment gateway to process payment

[0050] In the example, option 2 shown in Figure 11 is used to allow user credential based authentication and payment mechanisms presented by the selected CE 240 to be leveraged to complete the payment.

[0051] The flow embodied at steps 211–214 and 411 allows cryptocurrency payment capabilities available at the CE 240 to be leveraged. PG 230 initiates a cryptocurrency

request in step 211. CE 240 generates and returns a login URL against the request in step 212. This login URL is passed back to the customer 210 in step 213. The customer 210 authenticates and authorises the transfer at CE 240 in step 214 and cryptocurrency is transferred to PG's 230 wallet in step 411.

Notification of transaction result and fund settlement

[0052] Referring to Figure 11, at steps 501–503, customer 210 and merchant 220 are notified about the transaction. A request to sell the cryptocurrency in PG's 230 account at the CE 240 is submitted and the fiat currency amount is withdrawn in steps 504 and 505.

[0053] Funds in fiat currency are transferred from PG's 230 bank account to the merchant's 220 bank account in step 506 to complete the settlement process.

Example 2 - Non-tokenised QR code initiated direct processing at cryptocurrency exchange

Initialisation of payment process and selection of cryptocurrency exchange

[0054] This same process flow described in Example 1 above is used for this stage in this Example 2.

Authentication of customer and granting access to crypto payment gateway to process payment

[0055] In the example, option 3 shown in Figure 11 is used which allows QR code based authentication and payment mechanisms presented by the CE 240 to be leveraged to complete the payment.

[0056] Figure 9 is a mock-up of a QR code based authentication page presented by a CE 240 to trigger optional flow 3 in Figure 10. Flow option 3, which embodies steps 221-224 and 421, is similar to option 2 in Example 1, but incorporates a QR code based authentication mechanism. This is useful for customers 210 who prefer to complete the payment using a mobile device. PG 230 initiates a cryptocurrency request in step 221.

CE 240 generates and returns a code URL against the request in step 222. PG 230 renders a QR code based on the code URL and presents it to the customer 210 in step 223. The customer 210 scans the QR code in step 224 and authorises the payment, and cryptocurrency is transferred to PG's 230 wallet in step 421.

Notification of transaction result and fund settlement

[0057] This same process flow described in Example 1 above is used for this stage in this Example 2.

Example 3 – Tokenised payment with fraud and risk assessments

Initialisation of payment process and selection of cryptocurrency exchange

[0058] This same process flow described in Examples 1 and 2 above is used in this Example 3.

Authentication of customer and granting access to crypto payment gateway to process payment

[0059] In this Example 3, option 1 shown in Figure 10 is used for this stage. At step 201 the appropriate login URL is generated with token T2 based on the selected exchange. The customer 210 enters user credentials to the presented login screen.

[0060] At step 203, CE 240 authenticates and redirects the customer 210 back to PG 230 with an authorisation code and token T2. PG 230 extracts the authorisation code and uses to the authorisation code to request an access token T3. T2 is used to link T3 with the shopping basket details stored against T1.

[0061] These custom claims are encrypted by the PG 230 using the CE's 240 public key to ensure that it cannot be viewed/tampered with while it is passed through the customer's browser 210 to the CE 240. Once T2 is generated, the customer's browser 210 is redirected to the CE's 240 login page with T2.

Retrieval of wallets with sufficient balance and authorisation of payment

[0062] Token T3 is used to retrieve the customer's 210 list of wallets with cryptocurrency, their balances, and the conversion rate to a target fiat currency, in steps 301 and 302.

[0063] At step 303, PG 230 filters the list of wallets and returns only those that have sufficient balance to complete the payment, along with the balances and the conversion rate to the target fiat currency.

[0064] At step 304, the customer 210 selects a wallet W1 and authorises the payment in step 305.

Retrieval of transaction history of authorised wallet, anti-fraud assessments and perform transfer (payment) from authorised wallet

[0065] Referring to option 1 in Figure 10, at step 401, the PG 230 requests the transaction history of W1 using T3. The CE 240 returns transaction history of W1 at step 402. At step 403, the PG 230 retrieves all risk assessment NFTs related to the customer 210 profile 210. The customer 210 profile may be determined based on identification details retrieved from the CE 240.

[0066] At step 404, the PG 230 performs AML and anti-fraud assessments based on the shopping basket details, merchant's 220 category and returned transaction history. A decision is made at step 405 to proceed with or reject the transaction.

[0067] If risk assessment is successful, PG 230 issues a transfer request to send C1 from W1 to PG's 230 wallet at step 406. The CE 240 performs the requested transfer at step 407.

[0068] At step 408, a risk assessment NFT for the transaction is stored against the customer 210 profile.

Notification of transaction result and fund settlement

[0069] This same process flow described in Examples 1 and 2 above is used for this stage in this Example 3.

[0070] Embodiments of the present invention provide a system and related method that are both generally and specifically useful for providing a secure and compliant multi-cryptocurrency payment gateway.

[0071] Embodiments of invention advantageously provide a solution which allows consumers and merchants to be identified, and anti-fraud assessments to be performed when processing cryptocurrency-based payments. Merchants are identified when onboarding and provisioning an account at the payment gateway, consumers are identified using the KYC (Know Your Customer) and onboarding processes at the cryptocurrency exchange, and anti-fraud assessments are performed based on the transaction history of the customer's wallet, which is maintained at a cryptocurrency exchange.

[0072] Embodiments of the invention also provide the following advantages:

1. Allows payment gateways to be introduced to the cryptocurrency landscape. With currently available technology, merchants need to directly integrate with cryptocurrency exchanges via APIs to facilitate payments using cryptocurrency. The integration methods available with cryptocurrency exchanges are quite different from those used when processing credit card, debit card or stored value wallets. By introducing a cryptocurrency payment gateway, merchants are provided with an integration method that is the same as that used when accepting credit card payments from consumers.
2. Allows merchants to provide cryptocurrency as an option alongside other payment methods (eg, credit card, debit card or stored value wallets), to consumers.

3. Minimises or avoids the risk of fraudulently-obtained cryptocurrency being used in a transaction, by looking at the transaction history of the wallet of the consumer, and checking the source of the cryptocurrency.
4. A three token mechanism which allows the shopping basket details to be used together with the consumer's wallet history and provide an aggregate risk assessment score.
5. A settlement mechanism when accepting cryptocurrency payments by provisioning a digital credit card and then using the card scheme rails to transfer the funds to the relevant merchant's acquiring wallet.

[0073] Unless the context requires otherwise, the word "comprising" means "including but not limited to," and the word "comprises" has a corresponding meaning.

[0074] Any reference to prior art is not an admission that the prior art is common general knowledge.

[0075] The scope of the invention supported by the above examples is defined by the claims that follow.

Claims

1. A system, comprising:
 - a memory; and
 - a processor configured by instructions stored in the memory to:
 - receive, at a payment gateway, a payment request and shopping basket details of a customer from a merchant, wherein the payment request comprises a request for the payment gateway to pay a fiat currency amount to the merchant after an equivalent cryptocurrency amount has been transferred from a cryptocurrency wallet of the customer to a cryptocurrency wallet of the payment gateway;
 - generate a token representing the payment request;
 - store the token and the shopping basket details for subsequent processing of the payment request by the payment gateway;
 - provide an interface to the customer to select a cryptocurrency exchange to transfer the equivalent cryptocurrency amount from the cryptocurrency wallet of the customer to the cryptocurrency wallet of the payment gateway;
 - request the cryptocurrency exchange to sell the equivalent cryptocurrency amount in the cryptocurrency wallet of the payment gateway for the fiat currency amount;
 - receive a transfer of the fiat currency amount from the cryptocurrency exchange to the payment gateway;
 - notify the merchant and the customer that the payment request has been successfully processed by the payment gateway;
 - settle the payment request by transferring the fiat currency amount from the payment gateway to the merchant.
2. The system of claim 1, wherein the interface provided to the customer to select the cryptocurrency exchange comprises a login uniform resource locator (URL) of the cryptocurrency exchange.
3. The system of claim 1, wherein the interface provided to the customer to select the cryptocurrency exchange comprises a quick response (QR) payment code for the cryptocurrency exchange.

4. The system of claim 1, wherein the interface provided to the customer to select the cryptocurrency exchange comprises a first further token that includes the token representing the payment request, and wherein the first further token allows the customer to authorise the cryptocurrency exchange to send the payment gateway a second further token including the first further token that allows the payment gateway to retrieve a balance amount and a transaction history of the cryptocurrency wallet of the customer.
5. The system of claim 4, wherein the payment gateway performs a risk assessment for the payment request based at least in part on the shopping basket details, and the balance amount and the transaction history of the cryptocurrency wallet of the customer.
6. The system of claim 5, wherein if the risk assessment is satisfactory, the payment gateway uses the second further token to request the cryptocurrency exchange to transfer the equivalent cryptocurrency amount from the cryptocurrency wallet of the customer to the cryptocurrency wallet of the payment gateway.
7. The system of claim 5, wherein the payment gateway generates a non-fungible token (NFT) representing the risk assessment for the payment request.
8. The system of claim 7, wherein the payment gateway stores the NFT in a customer profile of the customer.
9. The system of claim 5, wherein the risk assessment may comprise one or both of an anti-money laundering (AML) risk assessment and a fraud risk assessment.
10. The system of claim 4, wherein the token representing the payment request, and the first and second further tokens, each comprise an encrypted JSON Web Token (JWT).
11. A method, comprising:
 - receiving, at a payment gateway, a payment request and shopping basket details of a customer from a merchant, wherein the payment request comprises a request for the payment gateway to pay a fiat currency amount to the merchant after an equivalent cryptocurrency amount has been transferred from a cryptocurrency wallet of the customer to a cryptocurrency wallet of the payment gateway;
 - generating a token representing the payment request;

storing the token and the shopping basket details for subsequent processing of the payment request by the payment gateway;

providing an interface to the customer to select a cryptocurrency exchange to transfer the equivalent cryptocurrency amount from the cryptocurrency wallet of the customer to the cryptocurrency wallet of the payment gateway;

requesting the cryptocurrency exchange to sell the equivalent cryptocurrency amount in the cryptocurrency wallet of the payment gateway for the fiat currency amount;

receiving a transfer of the fiat currency amount from the cryptocurrency exchange to the payment gateway;

notifying the merchant and the customer that the payment request has been successfully processed by the payment gateway;

settling the payment request by transferring the fiat currency amount from the payment gateway to the merchant.

12. A non-transitory machine-readable medium having stored thereon machine-readable instructions executable to cause a machine to perform operations comprising:

receiving, at a payment gateway, a payment request and shopping basket details of a customer from a merchant, wherein the payment request comprises a request for the payment gateway to pay a fiat currency amount to the merchant after an equivalent cryptocurrency amount has been transferred from a cryptocurrency wallet of the customer to a cryptocurrency wallet of the payment gateway;

generating a token representing the payment request;

storing the token and the shopping basket details for subsequent processing of the payment request by the payment gateway;

providing an interface to the customer to select a cryptocurrency exchange to transfer the equivalent cryptocurrency amount from the cryptocurrency wallet of the customer to the cryptocurrency wallet of the payment gateway;

requesting the cryptocurrency exchange to sell the equivalent cryptocurrency amount in the cryptocurrency wallet of the payment gateway for the fiat currency amount;

receiving a transfer of the fiat currency amount from the cryptocurrency exchange to the payment gateway;

notifying the merchant and the customer that the payment request has been successfully processed by the payment gateway;

settling the payment request by transferring the fiat currency amount from the payment gateway to the merchant.