

**USING A CONTACTLESS CARD TO SECURELY SHARE PERSONAL DATA
STORED IN A BLOCKCHAIN**

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application Serial No. 16/359,980, entitled “USING A CONTACTLESS CARD TO SECURELY SHARE PERSONAL DATA STORED IN A BLOCKCHAIN” filed on March 20, 2019. The contents of the aforementioned application are incorporated herein by reference in their entirety.

TECHNICAL FIELD

[0002] Embodiments herein generally relate to sharing data, and more specifically, to using a contactless card to securely share personal data stored in a blockchain.

BACKGROUND

[0003] Users often need to share personal data with merchants, government officials, and other entities. Using conventional techniques, however, often exposes more personal data than is needed. For example, when purchasing age-restricted items, only the age of the person needs to be provided. However, additional data such as the person’s name, address, and driver’s license number may be exposed when their driver’s license is scanned at the point of sale.

SUMMARY

[0003a] According to an aspect, there is provided a method comprising: receiving, by a verification service executing on a server from a mobile device, a digital signature, an encrypted request to provide a user data element to a merchant wallet address, and a user wallet address, wherein an applet of a contactless card generates the digital signature based on a private key of the contactless card, wherein the applet generates the encrypted request based on a first request received from a merchant device as part of a transaction; verifying, by the verification service, the digital signature based on a public key associated with the private key of the contactless card; decrypting, by the verification service, the encrypted request using the private key; receiving, by the verification service, the user data element; encrypting, by the verification service, the user data element using the public key to produce an encrypted user data element; and generating, by a node of a blockchain responsive to a second request received from the verification service, a block in the blockchain corresponding to the first request, the block comprising an indication of the verification of the digital signature, the encrypted user data element, the public key, the merchant wallet address, and the user wallet address.

[0003b] According to another aspect, there is provided a system, comprising: a processor and a memory storing instructions which when executed by the processor cause the processor to: receive, from a mobile device, a digital signature, an encrypted request to provide a user data element to a merchant wallet address, and a user wallet address, wherein an applet of a contactless card generates the digital signature based on a private key of the contactless card, wherein the applet generates the encrypted request based on a first request received from a merchant device as part of a transaction; verify the digital signature based on a public key associated with the private key; decrypt the encrypted request using the private key; receive the user data element; encrypt the received user data element using the public key to produce an encrypted user data element; and generate a block in a blockchain corresponding to the first request to provide the data element to the merchant wallet address, the block comprising an indication of the verification of the digital signature, the encrypted user data element, the public key, the merchant wallet address, and the user wallet address.

[0003c] According to another aspect, there is provided a computer-readable storage medium storing computer-readable program code executable by a processor to cause the processor to: receive, from a mobile device, a digital signature, an encrypted request to provide a user data element to a merchant wallet address, and a user wallet address, wherein an applet of a contactless card generates the digital signature based on a private key of the contactless card, wherein the applet generates the encrypted request based on a first request received from a merchant device as part of a transaction; verify the digital signature based on a public key associated with the private key; decrypt the encrypted request using the private key; receive the user data element; encrypt the received user data element using the public key to produce an encrypted user data element; and generate a block in a blockchain corresponding to the first request to provide the data element to the merchant wallet address, the block comprising an indication of the verification of the digital signature, the encrypted user data element, the public key, the merchant wallet address, and the user wallet address.

[0004] Embodiments disclosed herein provide systems, methods, articles of manufacture, and computer-readable media for using a contactless card to securely share personal data stored in a blockchain. In one example, a communications interface of a contactless card may receive, from a card reader of a merchant device, a request to provide a user data element to a wallet address associated with the merchant. An applet executing in a memory of the contactless card may encrypt, based on a private key stored in a memory of the contactless card, an indication of the user data element and the wallet address. The applet may generate, based on the private key, a digital signature for the request, and transmit, to a card reader of a mobile device by the communications interface of the contactless card, the digital signature and the encrypted indication of the user data element and the wallet address. The mobile device may transmit, to a verification service, the digital signature and the encrypted indication of the user data element and the wallet address. The verification service may verify the digital signature based on a public key associated with the private key of the contactless card. A node in a blockchain may generate a block in the blockchain corresponding to the request responsive to the verifying by the verification service, the block comprising indications of the verification of the digital signature, the requested data element, and the wallet address associated with the merchant. An encrypted data element corresponding to the user data element may be decrypted using a public key. The device of the merchant may

CLAIMS

1. A method, comprising:

receiving, by a verification service executing on a server from a mobile device, a digital signature, an encrypted request to provide a user data element to a merchant wallet address, and a user wallet address, wherein an applet of a contactless card generates the digital signature based on a private key of the contactless card, wherein the applet generates the encrypted request based on a first request received from a merchant device as part of a transaction;

verifying, by the verification service, the digital signature based on a public key associated with the private key of the contactless card;

decrypting, by the verification service, the encrypted request using the private key;

receiving, by the verification service, the user data element;

encrypting, by the verification service, the user data element using the public key to produce an encrypted user data element; and

generating, by a node of a blockchain responsive to a second request received from the verification service, a block in the blockchain corresponding to the first request, the block comprising an indication of the verification of the digital signature, the encrypted user data element, the public key, the merchant wallet address, and the user wallet address.

2. The method of claim 1, wherein the block in the blockchain further comprises an indication of a request token associated with the first request, wherein the user data element is one of a plurality of user data elements, each user data element corresponding to one or more personally identifiable attributes describing the user, the personally identifiable attributes comprising: (i) an age, (ii) a name, (iii) an address, (iv) an identification number, (v) one or more biometric identifiers, (vi) one or more account numbers, and (vii) an email address.

3. The method of claim 1, further comprising:

identifying, by the verification service, a plurality of blocks of the blockchain associated with a plurality of prior requests, the plurality of prior requests validated and fulfilled to provide user data elements of the user.

4. The method of claim 1, further comprising:

transmitting the second request by the verification service to the node of the blockchain, wherein the second request comprises the encrypted user data element, the indication of the verification of the digital signature, the public key, the merchant wallet address, and the user wallet address.

5. The method of claim 4, further comprising:

responsive to generation of the block, reading, by the merchant device, the block in the blockchain;

decrypting, by the merchant device based on the public key, the encrypted user data element; and

authorizing, by the merchant device, the transaction based on the decrypted user data element.

6. The method of claim 1, further comprising:

decrypting, by the verification service based on the public key, the encrypted user data element and the wallet address to validate an identity of the user.

7. The method of claim 1, wherein verifying the digital signature comprises decrypting the digital signature by the verification service based on the public key, wherein the digital signature comprises a hash value.

8. A system, comprising:

a processor; and

a memory storing instructions which when executed by the processor cause the processor to:

receive, from a mobile device, a digital signature, an encrypted request to provide a user data element to a merchant wallet address, and a user wallet address, wherein an applet of a contactless card generates the digital signature based on a private key of the contactless card, wherein the applet generates the encrypted request based on a first request received from a merchant device as part of a transaction;

verify the digital signature based on a public key associated with the private key;

decrypt the encrypted request using the private key;

receive the user data element;

encrypt the received user data element using the public key to produce an encrypted user data element; and

generate a block in a blockchain corresponding to the first request to provide the data element to the merchant wallet address, the block comprising an indication of the verification of the digital signature, the encrypted user data element, the public key, the merchant wallet address, and the user wallet address.

9. The system of claim 8, wherein the block in the blockchain is generated responsive to a second request, wherein the second request comprises the encrypted user data element, the indication of the verification of the digital signature, the public key, the merchant wallet address, and the user wallet address.

10. The system of claim 8, wherein the block in the blockchain further comprises an indication of a request token associated with the first request, wherein the user data element is one of a plurality of user data elements, each user data element corresponding to one or more personally identifiable attributes describing the user, the personally identifiable attributes comprising: (i) an age, (ii) a name, (iii) an address, (iv) an identification number, (v) one or more biometric identifiers, (vi) one or more account numbers, and (vii) an email address.

11. The system of claim 8, the memory storing instructions which when executed by the processor cause the processor to:

receive, from the merchant device, an indication that the transaction was authorized based on decrypting of the encrypted user data element stored in the block of the blockchain.

12. The system of claim 8, the memory storing instructions which when executed by the processor cause the processor to:

identify a plurality of blocks of the blockchain associated with a plurality of prior requests, the plurality of prior requests validated and fulfilled to provide user data elements of the user.

13. The system of claim 8, the memory storing instructions which when executed by the processor cause the processor to:

decrypt the digital signature based on the public key to verify the digital signature, wherein the digital signature comprises a hash value.

14. The system of claim 8, the memory storing instructions which when executed by the processor cause the processor to:

decrypt, based on the public key, the encrypted user data element and the wallet address to validate an identity of the user.

15. A computer-readable storage medium storing computer-readable program code executable by a processor to cause the processor to:

receive, from a mobile device, a digital signature, an encrypted request to provide a user data element to a merchant wallet address, and a user wallet address, wherein an applet of a contactless card generates the digital signature based on a private key of the contactless card, wherein the applet generates the encrypted request based on a first request received from a merchant device as part of a transaction;

verify the digital signature based on a public key associated with the private key;

decrypt the encrypted request using the private key;

receive the user data element;

encrypt the received user data element using the public key to produce an encrypted user data element; and

generate a block in a blockchain corresponding to the first request to provide the data element to the merchant wallet address, the block comprising an indication of the verification of the digital signature, the encrypted user data element, the public key, the merchant wallet address, and the user wallet address.

16. The computer-readable storage medium of claim 15, wherein the block in the blockchain is generated responsive to a second request, wherein the second request comprises the encrypted user data element, the indication of the verification of the digital signature, the public key, the merchant wallet address, and the user wallet address.

17. The computer-readable storage medium of claim 15, wherein the block in the blockchain further comprises an indication of a request token associated with the first request, wherein the user data element is one of a plurality of user data elements, each user data element corresponding to one or more personally identifiable attributes describing the user, the personally identifiable attributes comprising: (i) an age, (ii) a name, (iii) an address, (iv) an identification number, (v) one or more biometric identifiers, (vi) one or more account numbers, and (vii) an email address.

18. The computer-readable storage medium of claim 15, storing computer-readable program code executable by the processor to cause the processor to:

receive, from the merchant device, an indication that the transaction was authorized based on decrypting of the encrypted user data element stored in the block of the blockchain.

19. The computer-readable storage medium of claim 15, storing computer-readable program code executable by the processor to cause the processor to:

decrypt the digital signature based on the public key to verify the digital signature, wherein the digital signature comprises a hash value.

20. The computer-readable storage medium of claim 15, storing computer-readable program code executable by the processor to cause the processor to:

decrypt, based on the public key, the encrypted user data element and the user wallet address to validate an identity of the user.